Project 4 - Entrepreneurism & Ethics
1: Ethical Business Plan

1.A. - Pathfinder

1.B. Long Term Vision Statement

- 1.B.1: To Automate driving for previous generation cars to help keep them out of landfills. We also want to make roads safer by reducing the amount of unsafe human drivers from distractions and drunk driving which cause many preventable fatalities every year.
- 1.B.2: The idea came from the current climate where AI is very topical and there is a lot of discussion about its consequences and how society might change as a result of new technology like LLMs.
- 1.B.3: The purpose of our company is to introduce previous generation cars that may not have self driving functions to software and hardware that will automate driving. We value reliability, functionality, and safety. Our mission is to install self driving hardware for people who may desire or want self driving without actually needing to buy a new car.
- 1.B.4:
  - How does Pathfinder reduce preventable accidents and extend the life of older cars?
  - What engages our passions?
  - How can we install self driving technology?

  Our OKRs: Ensure product meets Ethics and Privacy standards - Luka, Customer Satisfaction - Angel, and Safety and Reliability - Ivan

  Ensure product meets Ethics and Privacy standards
  - develop standards with government/regulating bodies

1.C.1. OKR 1 (Luka)

1.C.1.1: ONE Objective and Key Result
　　Objective: Ensure product meets Ethics and Privacy standards.
　　Key Result: Develop and implement data privacy standards and security protocols compliant with all applicable national and state laws (e.g., CCPA, GDPR standards for data protection) and achieve 100% anonymization/aggregation of non-safety-critical personal data prior to server storage within the first year.

Our consumer base is very broad across many demographics such as race, gender and interests because of the widespread need for economical, efficient travel. It would largely cater to lower incomes because of its appeal for extending the lifespan of existing cars, however. Higher income individuals may be more interested in buying new vehicles altogether.

1.C.1.2: Metrics with Experimentation

The success of the OKR will be measured by two metrics: Legal Compliance and Data Security Performance.

Metric 1: Legal Compliance Audit Score
Explicit Metric: Achieve an external, independent legal audit score of 100% compliance with all personally identifiable information (PII) handling and storage regulations (including, but not limited to, data breach notification protocols and user consent mechanisms) applicable in Pathfinder's operational territories.

Experiment: Legal Compliance Audit
Auditor Engagement: An external, specialized legal firm (with expertise in data privacy law, e.g., CCPA and GDPR) will be contracted to perform a formal audit of Pathfinder's data handling protocols.

Audit Scope: The firm will review:
The customer consent agreement (EULA) for clarity and transparency on data collection.
The data flow architecture: tracing data from the in-car unit to the server.
The data retention and destruction policies.
The breach notification plan.
The mechanisms for user data access and deletion requests.

Evaluation: The legal firm will issue a formal report. The OKR is achieved only if the report states 100% compliance and zero critical legal flaws in the simulated requests.

Metric 2: Data Anonymization Rate
Explicit Metric: 100% of all customer-specific driving data (telemetry, location history) stored on company servers (cloud storage) must be anonymized or aggregated so that it cannot be reasonably re-identified as PII, as validated by an internal data science team.

Experiment: Re-Identification Stress Test
A sandbox environment containing a subset of the first 1,000 users' driving data—after it has undergone the anonymization/aggregation protocol—will be created. This data set will exclude any explicitly stored PII (like customer name, address).

Evaluation: The OKR is successful only if a technical team attempting to reverse engineer the data achieves a 0% re-identification rate over a three-month testing window. If re-identification is successful for even a single record, the anonymization protocol is considered a failure, and engineering must be halted until a more robust k-anonymity or differential privacy technique is implemented.

1.C.1.3: Ethical Impact(s)/Issue(s)

The core product's continuous, sensitive data collection (location, speed) poses high risks. Even 100% anonymization is an illusion (Strava case [1]), as data can be de-anonymized. Function Creep (Scenario 2) threatens to exploit this data for profit, violating the ethical mandate. This results in High Privacy/Rights Risk for customers and High Financial/Interest Risk for Pathfinder.

Stakeholder	Financial Risk	Privacy Risk	Conflicting Interest Risk	Violation of Rights Risk
Consumer (User)	Mid	High	High	High
Company (Pathfinder)	High	Low	Mid	Low
Insurers	Mid	Low	High	Mid

Customer stakeholder:
This user faces a high risk for privacy and violation of rights because even anonymized location data and other such information (driving habits, location history) can be de-anonymized and used for profiling and algorithmic discrimination. This creates a high conflict of interest between the user's need for privacy and the company's profit motives, resulting in mid-financial risk from potential impacts on services like insurance rates.

Company/Pathfinder stakeholder:
The company faces a high financial risk due to the devastating potential for regulatory fines (like GDPR/CCPA) and costly lawsuits if the data anonymization protocols fail. The conflicting interest risk is mid, arising from the internal tension between engineering teams that want rich data for product improvement and the ethical mandate for strict data minimization.

Future business partners/insurers stakeholder:

These third parties have a high conflict of interest, as their need for detailed behavioral data to maximize profit directly opposes the user's right to privacy. If they utilize improperly sourced data for discriminatory pricing, they assume a mid violation of rights risk and face mid-financial risk from resultant public backlash and legal challenges.

1.C.1.4: Ethical Safeguards

To address the OKR on "Ethics and Privacy Standards" and mitigate Privacy Illusion and Function Creep, Pathfinder will implement a two-part safeguard, supported by the principles of Privacy by Design [2].

1. Real-Time Data Transparency UI:
The in-car and mobile app will feature an always-accessible "Data Status" screen. This UI provides visual indicators of real-time data collection and clear status labels (e.g., "Data Anonymized: 100%"). Crucially, it includes a one-click User Control to adjust consent and initiate an immediate data purge. This counters the "Privacy Illusion" by making data flow comprehensible to the user.

2. Mandatory Data Minimization Review:
An external Ethical Expert/Data Minimization Expert will be hired to audit the system and ensure the least amount of PII is collected. Any proposal for new data use ("Function Creep") must pass through a formal Data Protection Impact Assessment (DPIA) and be signed off by this expert, creating an external, expert check [3].

Effectiveness Metrics:

Transparency: 90% correct answers on a mandatory 3-question in-UI quiz, measuring customer understanding of the data policy.

Minimization: Zero-instances of unauthorized data access requests from internal business units (marketing, sales) not covered by a pre-approved DPIA.

1.C.1.5: References

[1] MORRIS, D. Z. 2018. Strava's global heatmap data reveals sensitive military base locations. Fortune. Retrieved from https://fortune.com/section/magazine/

[2] CAVOUKIAN, A. 2011. Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario. Retrieved from https://www.linkedin.com/pulse/7-principles-pretty-good-documentation-tam%C3%A1s-varga-8 abjf

[3] ACM US Public Policy Council. 2017. Statement on algorithmic transparency and accountability. Retrieved from https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf

1.C.2 OKR 2(Ivan)

1.C.2.1: One Objective and Key Result

The company wishes to establish a 99% reliability rate of safety in their autonomous system in the first year of operations. The key result is that there will be no more than one incident attributed to the system per one hundred thousand miles of car activity. This goal enables the company to promote safe driving, create public confidence that this system of transportation is safe to the users and limits user exposure to harm. The stakeholders of this venture are drivers between 25 and 55 years of age, government regulators and auditors including NHTSA, insurance companies, and the software and hardware teams that are responsible for system reliability. Each stakeholder serves a specific function to ensure that the product continues to meet the highest in safety standards.

1.C.2.2: Metric(s) with Experimentation

Pathfinder will measure its success through the measurement of parameters designed to qualify the successful outcomes of success. These measurements are two-fold and consist of a measurement for the autonomous incident rate (AIR) which will be a count of per accident to number of miles with automobiles driving themselves in good conditions on up to 100,000 miles driven. This measurement will take place in a six month pilot exploration of 500 automobiles in a variety of conditions. The results of these autonomous cars will be verified by independent auditors to substantiate the validity of the conclusions. The other mode employed will be a driver confidence index (DCI) which will measure how secure the users felt in using Pathfinder, and it will be based on a survey of the users that will ask questions such as "how safe did you feel while Pathfinder was driving?" The goal of this company is that this confidence rating be in larger than 90%. Both measurements will be overseen by an expeditious collection of measurable results and the use of real time analytics to help refine the safety results of the objective.

1.C.2.3: Ethical Impact(s)/Issue(s)

An ethical concern that is paramount in safety and reliability involves algorithmic accountability; that is if a driverless automobile experiences a mishap and causes harm or damage, who is accountable, the driver user, the manufacturer of the car or the developer of the software? Similar ethical dilemmas were witnessed in the case of March 2018, Uber Technologies, Inc. v. Tempe

Police Department, where an Uber self-driving test vehicle fatally injured a pedestrian thus showing inadequate supervision and safety testing procedures in the systems capabilities [1].

Stakeholder	Financial Risk	Privacy Risk	Conflicting Interest Risk	Violation of Rights
Customer	Mid	Low	High	Mid
Company	High	Mid	Mid	High
Regulator	Low	Low	Mid	Low
Supplier	Mid	Low	Low	Low

A consideration of the ethical problems that users of the products face world an interaction of a moderate resulting in financial harm with safety and potentially fatal, resulting in great conflicting interest when matters of control are taken over by automation. The company faces high financial risks and potentially bad publicity with active rights caused by location of the time of exposure due to systems failing at a critical time. The regulators, holding both the governmental purse strings and general public interest, weigh considerations of safety as against innovation, and the supplier bears low risk save for present problems relating to the public. This indicates the vertical extent of risks bringing accountability and transparency into focus with safety and ethics also involved.

1.C.2.4: Ethical Safeguards

In order to reduce the respective risks Pathfinder will protect each vehicle with a safe mode of event logging system incorporated into every vehicle which will advise if the system experiences some failure and resultant actions leading to an accident, the record, being encrypted and able to document what type of circumstance exists and permit indemnification and blame. The system will make use of dual-sensor redundancy in its workings of automation thus radar and optical interactions will have confirmation as to result pending major steps being taken somewhat along the lines of FAA standards of aviation safety [2]. Pathfinder will also elect to form an ethics and safety review board with members of its engineers along with the established ethicists from time to time to audit said data every three months as time permits. Feedback from any exploratory

usage and survey forms relating to users of the various Pathfinder products might allow for systems improvement in due course of time with ethical and reliability of control and use of said technology forming a tangible base.

1.C.2.5: References

- [1] A. Smith. 2019. *The Uber Self-Driving Car Fatality: Who's Responsible? Journal of Technology Ethics* 14, 2 (2019), 45–57.
- [2] Federal Aviation Administration. 2021. *Aircraft System Redundancy Standards for Safety Certification.* U.S. Department of Transportation, Washington, D.C.

1.C.3 OKR 3(Anjel)

1.C.3.1: Objective and Key Result :

Pathfinder aims to achieve exceptional customer satisfaction by ensuring that its retrofit system delivers a seamless, safe, and reliable user experience for all drivers. The company's key result is to reach a 90% customer satisfaction rating by the end of its first operational year, measured through post install surveys and user feedback, while maintaining a system malfunction rate below 5%. This goal emphasizes Pathfinder's commitment to quality performance and trust between customers and the technology.

Pathfinder's customers include middle class car owners aged 25 through 65, representing diverse genders, races, and backgrounds, who are interested in affordable self driving solutions and environmental sustainability. Their satisfaction depends on the reliability of the system, ease of use, and responsive support services. Automotive technicians and partner garages play a key role as they handle installations that directly affect customer experience. Insurance companies also benefit from safer driving behavior, while government transportation agencies view high satisfaction rates as indicators of readiness for broader regulatory support. Computation for driving decisions occurs locally within the vehicle's hardware, while aggregated satisfaction and performance data are securely stored on Pathfinder's cloud servers to inform ongoing improvements. Through collaboration among customers, technicians, insurers, and Pathfinder's engineers, the company ensures that user experiences drive the evolution of its technology.

1.C.3.2: Metric(s) with Experimentation:

To measure the success of Pathfinder's customer satisfaction OKR, we will use two main metrics, a Customer Satisfaction Survey and a System Reliability Report. The customer satisfaction survey will be administered one month after installation to a sample of 300 users from diverse ages, incomes, and racial backgrounds. Users will rate their experience on a 1 through 10 scale across categories such as ease of use, reliability, and customer support. The

overall satisfaction score will be calculated as the average percentage across all responses. Success will be defined as an average score of 9/10 or higher.

System reliability will be tracked automatically through Pathfinder's onboard diagnostics in 500 vehicles. Each car will log all autonomous trips, flagging any malfunctions, disengagements, or driver takeovers. These data points will be processed locally for safety decisions, then uploaded to Pathfinder's secure cloud for analysis. The malfunction rate will be calculated monthly as the percentage of failed trips relative to total trips, with a success threshold set at 5% or lower. The combined data from user surveys and reliability metrics will be reviewed quarterly to assess customer satisfaction trends and guide software and hardware improvements.

1.C.3.3: Ethical Impact(s)/Issue(s):

Pathfinder's customer satisfaction OKR introduces ethical issues related to privacy, transparency, and safety responsibility. Since satisfaction data comes from both user surveys and driving performance logs, there is potential misuse of sensitive data such as location and driving behavior. A comparable ethical concern arose with Tesla's Autopilot system, where the company faced criticism for releasing semi-autonomous software that users might over trust without full awareness of its limitations. Vincent (2018) argues that promoting technology as "Autopilot" without sufficient safety safeguards or public transparency violates ethical standards of responsibility and honesty. Similarly, Pathfinder must ensure data use, testing, and marketing practices remain transparent and prioritize driver safety over reputation metrics.

Stakeholder	Financial	Privacy	Conflicting Interest	Violation of Rights
Customer (Driver)	Low	High	Medium	Medium
Technicians/ Installers	Medium	Low	Medium	Low
Insurance Companies	Low	Medium	High	Low
Government Agencies	Low	Low	Medium	Low
Pathfinder Company	High	Medium	High	Medium

Drivers face high privacy risk since satisfaction tracking involves personal driving and behavioral data. Technicians face medium financial risk if improper installation leads to accidents. Insurance companies pose high conflict of interest risk, as they may exploit driving

data to adjust premiums. Government agencies have low privacy risk but must balance innovation with regulation. Pathfinder bears high financial and ethical risk if customer data or safety claims are mishandled.

1.C.3.4: Ethical Safeguards

To reduce the ethical risks in Pathfinder's customer satisfaction OKR, the company will apply three main safeguards.

Pathfinder vehicles will display a visual dashboard light and a brief voice alert whenever data collection is active, ensuring users know when their information is being recorded. A UI/UX designer and ethics consultant will codesign this system, and effectiveness will be measured through user feedback showing at least 95 % awareness of the indicator's purpose.

All data will be encrypted and anonymized before leaving the vehicle. Annual third party audits will verify compliance with ethical and data protection standards outlined in the ACM Code of Ethics (Gotterbarn et al., 2018). Success will be measured by maintaining zero privacy incidents per year.

To prevent biased satisfaction metrics, survey participation will include balanced representation across age, gender, and technical literacy groups. A small data ethics team will oversee sampling and measure success by keeping demographic deviation under 10 % of national averages. These safeguards ensure Pathfinder's operations remain transparent, fair, and respectful of user privacy while advancing safe self-driving innovation.

1.C.3.5: References:

Gotterbarn, D., Miller, K., and Rogerson, S. 2018. ACM Code of Ethics and Professional Conduct. Association for Computing Machinery. October 13, 2025, https://www.acm.org/code-of-ethics

Vincent, K. 2018. Ethical Implications: The ACM/IEEE-CS Software Engineering Code applied to Tesla's "Autopilot" System. October 13, 2025, https://arxiv.org/abs/1901.06244

Section 2: Cultural Policy

2.A. Core Values

Pathfinder aims to be the definitive leader in responsible, retrofit automotive safety and sustainable technology. We will set the standard for ethical reliability and sustainability. Every decision, from design to deployment, must prioritize user safety, data privacy, and public accountability. We commit to functionality rigorously tested to exceed the highest existing safety standards, ensuring the system is dependable and trustworthy across all driving conditions. Our processes emphasize transparency and proactive engagement with regulatory bodies to build public confidence.

Sustainable Excellence centers on the entire lifecycle of a vehicle. Our culture is driven by the goal of keeping older, well-maintained cars productive, relevant, and out of landfills. We

champion an innovative approach that extends car utility through retrofit automation, not replacement. This demands continuous learning, rigorous compliance, and uncompromising quality assurance in all practices. Team members must embody this commitment to longevity and responsible technology, defining Pathfinder by the responsible decades of use we inject back into existing vehicles.

2.B. Motivation

We love the profound, tangible impact of our mission: creating safer roads and achieving a smaller environmental footprint by prolonging the useful life of vehicles. We are passionately driven to bridge the technology and economic gap, enabling access to advanced safety features for car owners who cannot afford a new vehicle. Our core fulfillment comes from proving that genuine innovation can be revolutionary, fiscally sound, and environmentally responsible—automating driving without demanding total automotive replacement. We are energized by engineering complex, reliable systems that deliver simplicity and unparalleled safety, validating our hands-on approach.

We are aware of the catastrophic potential for technology failure when human life and safety are at stake. This drives our intense focus on redundant safety systems, rigorous simulation, and comprehensive real-world testing. We also fear breaking the relationship of trust with the public if we fail to execute our ideals regarding user data privacy or neglect proactive engagement with governing bodies. This fear compels every employee toward uncompromising due diligence.

2.C. Summary

We champion reliability, safety, and sustainability.

Section 3: Ethics Policy

3.A. The 5 Commitments are: (1) Data Privacy and Minimization, (2) Algorithmic Accountability and Explainability, (3) Safety First Engineering, (4) Environmental Responsibility, and (5) Fairness, Accessibility, and Non-Discrimination. Combined these 5 Commitments comprise the foundational ethical framework for Pathfinder and guide each of the Company's decisions throughout Product Development, Deployment and Long-Term Maintenance.

1. Data Privacy and Minimization

Pathfinder will only gather the least amount of data required to enable the safe operation of the Automated Driving System. Personal and Behavioral Data must undergo Anonymization and Encryption prior to being transferred off the Vehicle Hardware. Data collection will occur transparently with Real-Time Indicators when data is collected or stored. Users will retain control over their Data consistent with the CCPA and GDPR including Access, Erasure,

Modification, etc. under no circumstances will Pathfinder Share, Sell, License, Distribute any data of User Driving Behavior to Insurers, Advertisers, Law Enforcement, Third Parties without Explicit Consent which may be Revoked.

This Policy was created to Protect Users from Function Creep, Discriminatory Profiling and Unintended Secondary Uses of their Data.

2. Algorithmic Accountability and Explainability

Pathfinder believes that Automated Systems should be Traceable, Reviewable, Accountable. All AI Models utilized within the Driving System will undergo Regular Audits for Bias, Disparate Impact, Harmful Failure Modes by both Internal Engineers and External Ethics Auditors. A Structured "Incident Explainability Standard" will require Engineers to create Clear, Human-Readable Reports explaining System Decisions resulting from Near-Miss or Accident events. Pathfinder Rejects the Black Box Approach to AI and instead is committed to Transparency regarding How Driving Decisions are Made, Validated and Improved. This allows Regulators, Customers, Technicians to Evaluate the Safety of the System.

3. Safety First Engineering

Preventing Harm is Pathfinder's Most Important Ethical Obligation. Pathfinder adopts the Engineering Philosophy of Aviation: Redundancy, Verification, Independent Review. Mandatory requirements include dual-sensor redundancies, automated fail-safe modes, encrypted event logs, and continuous real-time system monitoring. No Software Update regardless of how minor will be Deployed without Rigorous Simulation Testing and Third Party Review to Minimize Risk of System Failure in Real-World Driving Environments. Safety Standards will Always pass Market Deadlines, Revenue Goals, Competitive Pressure, Investor Expectations. Pathfinder Employees are Encouraged and Required to Halt Production/Deployment if Potential Safety Risks Exist.

4. Environmental Responsibility

Pathfinder Exists to Extend the Lifespan of Older Vehicles and Reduce their Environmental Impact. Pathfinder has committed to Sustainable Hardware Sourcing, Responsible Supply Chain Practices, and Minimizing Electronic Waste. All Hardware Components Must be Recyclable or Recoverable, and Partner Installers Must Follow Strict Sustainability Guidelines. Pathfinder Recognizes that Ethical Technology Requires a Sustainable Lifecycle From Material Extraction to End-of-Life Disposal.

5. Fairness, Accessibility & Non-Discrimination

Our Technology Must Serve the Public Equitably. Pathfinder will Design All User Interfaces, Customer Support Systems, and Algorithmic Models with Fairness Assessments to

Prevent Discriminatory Outcomes Based on Race, Gender, Income, Disability Status or Geographic Location. We have Committed to Providing Retrofit Options at Affordable Price Tiers to Allow Low-Income and Working-Class Families who are Disproportionately Priced Out of New Self-Driving Cars Access to Safer Transportation. Fairness in Deployment is Not a Marketing Choice, it is a Core Ethical Requirement.

3.B. The Ethics Board of Pathfinder, Inc., will be composed of three members who have combined academic and professional experience in AI, Autonomous Systems, Cybersecurity and Applied Ethics. The primary function of the board is to provide oversight, review significant decision making by Pathfinder and identify potential "blind spots" for the organization as it relates to ethical considerations and to ensure that Pathfinder continues to adhere to its mission of Safety, Privacy and Public Trust.

1. Dr. Timnit Gebru — AI Ethics Researcher and founder of Distributed AI Research Institute (DAIR)

Dr. Timnit Gebru is an internationally recognized leader in her field due to her pioneering work in the areas of algorithmic fairness, transparency in AI systems, and the social implications of large-scale machine learning models. She previously co-leader of Google's Ethical AI Team and published numerous papers on topics related to bias, power structures and the social impact of AI technology. We selected Dr. Gebru because her body of research directly supports Pathfinder's main challenge areas – data privacy, algorithmic accountability, and anti-discrimination — and provides us with assurance that our models are both technically robust and socially responsible. Dr. Gebru's membership on the board gives us confidence that we will never overlook the impact of our technology on humans.

2. Fei-Fei Li — Professor of Computer Science at Stanford University and Co-Director of the Stanford Human-Centered AI Institute.

Dr. Fei-Fei Li is one of the world's top researchers in computer vision, machine learning and human-centered design. She was a key figure in developing ImageNet and has spent the last decade working to ensure that AI systems were developed using an ethical, multi-disciplinary approach. As one of the foremost experts in perception systems, Dr. Li will help guide our development of self-driving vehicles through accurate and interpretable visual recognition. Dr. Li represents the principles of "AI for people", and we believe she embodies the spirit of protecting human life while serving the public interest. Additionally, Dr. Li has extensive experience working to build partnerships among policymakers, engineers, and communities, which will assist us in navigating our regulatory relationship.

3. Alex Stamos — former Facebook Chief Security Officer and current director of the Stanford Internet Observatory

Alex Stamos is considered to be one of the most experienced and respected cybersecurity leaders in the technology industry. He has successfully managed large-scale data security systems during his tenure at Facebook and Yahoo. Based upon this experience, Mr. Stamos is uniquely qualified to oversee the data protection, anonymization protocols, breach preparedness, and long-term privacy infrastructure of Pathfinder. We selected Mr. Stamos based upon the fact that our autonomous vehicles will be collecting extremely sensitive data, such as location and behavioral telemetry, and the consequences of a breach could be devastating. In addition, Mr. Stamos' background assures us that our data infrastructure will remain secure against hacking, unauthorized access and manipulation. Stamos is well known for confronting difficult ethics questions within the technology industry and assists in reinforcing Pathfinder's commitment to transparency and honesty.

Section 4: YouTube Presentation

Section 5: References

Gotterbarn, D., Miller, K., and Rogerson, S. 2018. ACM Code of Ethics and Professional Conduct. Association for Computing Machinery. October 13, 2025, https://www.acm.org/code-of-ethics

Vincent, K. 2018. Ethical Implications: The ACM/IEEE-CS Software Engineering Code applied to Tesla's "Autopilot" System. October 13, 2025, https://arxiv.org/abs/1901.06244

A. Smith. 2019. *The Uber Self-Driving Car Fatality: Who's Responsible? Journal of Technology Ethics* 14, 2 (2019), 45–57.

Federal Aviation Administration. 2021. *Aircraft System Redundancy Standards for Safety Certification.* U.S. Department of Transportation, Washington, D.C.

MORRIS, D. Z. 2018. Strava's global heatmap data reveals sensitive military base locations. Fortune. Retrieved from https://fortune.com/section/magazine/

CAVOUKIAN, A. 2011. Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario. Retrieved from https://www.linkedin.com/pulse/7-principles-pretty-good-documentation-tam%C3%A1s-varga-8abjf