Supporting Documentation

Introduction:

The PET Advisor is designed to assist organizations in identifying and implementing appropriate privacy-preserving technologies for their specific data use cases. The tool does not assume prior expertise in privacy or legal compliance. Instead, it guides users through an interactive questionnaire that captures key aspects of their organization's technical environment, data handling practices, and regulatory obligations.

The questionnaire comprises 27 questions covering areas such as system architecture, data sensitivity, risk tolerance, and legal jurisdiction. After finishing the questionnaire, PET Advisor will recommend the top two most suitable techniques. These include Differential Privacy, Secure Multi-Party Computation, Trusted Execution Environments, Synthetic data generation, K-anonymity/L-diversity, and Cryptographic protocols, along with applicable legal frameworks such as HIPAA, GDPR, or CCPA. After receiving recommendations, users can access an implementation wizard with targeted follow-up questions and detailed setup guidance for each suggested technology.

The following will introduces the techniques and implementation details:

Anonymization Techniques

K-anonymity, l-diversity, and t-closeness. When the dataset includes quasi-identifiers (e.g., age, ZIP code,wage) the risk of re-identification is high, these techniques are ideal. It suits public health data and other record-level data that are intended for the public. Examples can be government census data and covid-19 data.

K-Anonymity ensures that each released record is indistinguishable from at least k-1 others based on key quasi-identifier. l-Diversity ensures that within each group of indistinguishable records, there is diversity in the sensitive attributes. T-Closeness adds a further check: the distribution of sensitive values in any group must be close to the overall distribution, minimizing skew attacks.

Example scenario:

In a public health dataset with age, ZIP code, gender, and COVID-19 status, suppose there's a 33-year-old female in ZIP 10027. If she's the only one with that combination, she is easily identifiable. *k-Anonymity* might generalize age to 30–40 and ZIP to 1002*, grouping her with at least four others. But if all in the group are COVID-positive, her status is still exposed. *l-Diversity* ensures varied outcomes (some positive, some not) in the group. *t-Closeness* goes further by keeping group distributions similar to the overall population, e.g., maintaining a 50/50 positive/negative ratio.

Practical implications:

k-Anonymity prevents simple re-identification via linkage attacks and retains utility in certain fields. It is fast and inexpensive. However, it lacks formal mathematical privacy guarantees, cannot guard against attackers with background knowledge, and requires generalization that may reduce usefulness for granular analysis.

Differential Privacy (DP)

Differential Privacy (DP) applies when datasets involve sensitive individual-level data and will be used for statistical analysis or repeated querying. It is suited for public records, ML model training, or aggregate statistics results. DP works by adding noise to the output of a query, ensuring that no single individual's data has a significant effect on the result. The key parameter is the privacy budget, denoted by epsilon (ε) — smaller values of ε mean stronger privacy but more noise, while larger ε values provide more accurate results but weaker protection.

DP has two main models:

- Central DP: Raw data is held by a trusted central, and noise is added to aggregate results before release.
- Local DP: Each individual processes their own data before it is collected, so the central server never sees raw inputs.

Example scenario:

A tech company wants to publish average salaries by department for a diversity transparency report. Instead of releasing the exact average , the system adds random noise to the result based on a chosen ε value. If analysts make hundreds of such queries, each one consumes part of the daily privacy budget, and eventually the privacy budget will run out and the protection will go low.

Practical implications:

Differential Privacy prevents re-identification attacks even if an attacker knows background information about individuals. It is effective in where many small queries are made or data is accessed repeatedly. The trade-offs are the noise may reduce accuracy and managing the privacy budget requires careful planning. Also, Local DP often requires significantly more noise than Central DP to maintain similar protection levels. DP is a strong solution when privacy must be guaranteed mathematically, especially in high-risk use cases. It's more complex and resource-intensive than k-anonymity.

Secure Multi-Party Computation (MPC)

MPC is used when sensitive data is distributed across multiple parties who need to compute results without revealing their private inputs. It's ideal for scenarios like cross-institution research, collaborative fraud detection, or joint financial analysis. MPC enables two or more parties to jointly compute over combined datasets using techniques like secret-sharing and secure aggregation without ever exposing raw data. Only the final result is revealed.

Example scenario:
Three competing banks want to jointly calculate how many customers across all three institutions have defaulted on loans without revealing individual customer records. Using MPC, each bank splits its internal default list into encrypted shares and shares them with the others. A secure computation protocol aggregates these without exposing any raw records, and only the final total number of defaults is revealed.

Practical implications:

MPC offers robust security guarantees, even when some parties are semi-honest (follow the protocol but try to learn information). However, it has computational overhead, requires coordination, and only protects against collusion up to a threshold *(t)*. It does not add noise or protect against inference from final outputs. MPC is valuable when no single party should have full access to sensitive data. However, it does not protect against collusion beyond the agreed threshold t.MPC is best combined with Differential Privacy to protect both the inputs and the final results.

Legal and Policy Compliance

Our decision-making tool considers legal and policy frameworks such as GDPR, HIPAA, COPPA, and etc. This is to ensure our recommendations closely follow and comply with current laws and regulations. Each law governs specific types of data and user populations, and the tool flags these conditions to prioritize legally permissible techniques.

HIPAA governs personal health information in the U.S. healthcare sector. When detected, we recommend HIPAA compliance checklists, along with Differential Privacy or anonymization techniques (e.g., k-anonymity) for de-identification.

GDPR, which protects data of individuals in the EU/EEA, emphasizes data minimization, consent, and user control.

CCPA/CPRA, relevant to California residents, focuses on consumer rights like opt-out and deletion.

ails.FERPA applies to student education records in federally funded institutions.

COPPA covers data about children under 13. To protect minors, we suggest strong Differential Privacy safeguards and clear parental consent tracking mechanisms.

FOIA, which governs access to federal agency records, often intersects with de-identification for public releases.

Synthetic Data Generation

Synthetic data generation involves creating artificial datasets that mimic the statistical properties of real data, often using machine learning models like GANs or VAEs. The goal here is to preserve utility for tasks like testing, training, or analysis, without exposing real user data.

Example scenario:
A fintech startup wants to develop a fraud detection model without exposing sensitive transaction records. By training a GAN model on internal datasets, they can generate synthetic data that reflects real patterns but contains no actual user records, enabling model development with reduced privacy risk.

Practical implications:
Synthetic data offers strong privacy potential , especially when combined with DP during model training, but sometimes it varies. Some poorly trained models may produce low-utility or unrealistic outputs, while overly realistic ones may inadvertently leak sensitive patterns. Our tool recommends synthetic data when high privacy is required but raw data cannot be shared, especially for internal ML prototyping or software testing. It's best used where the cost of incorrect inference is low, or as a supplement to other PETs.

Trusted Execution Environment

TEEs are hardware-based isolation mechanisms that allow sensitive computations to be securely executed inside protected enclaves (e.g., Intel SGX, ARM TrustZone). The operating system and other software outside the enclave cannot access the data or the computation being performed. So it is like a secure vault inside a computer's processor. When sensitive data needs to be processed—like passwords, health records, or financial info—it goes into this vault.

Example scenario:
A cloud analytics provider offers clients the ability to run some encrypted data processing jobs using Intel SGX-enabled servers. Sensitive data is decrypted and processed entirely within a secure enclave, and only final results are returned, reducing exposure risk.

Practical implications:
TEEs provide strong input protection without adding noise, making them ideal when exact results are needed and data sensitivity is high. They also reduce latency compared to cryptographic methods like MPC. However, they require specialized hardware, and recent vulnerabilities have exposed risks of side-channel attacks. Our tool recommends TEEs when real-time processing is required, trust in the hardware provider exists, client's willing to pay for the specialized hardware, and noise-based privacy is too disruptive for accuracy.

Structure and Logic

Our interactive questionnaire is built around a dynamic scoring system. Each question in the survey corresponds to a specific privacy consideration (like data sensitivity, real-time requirements, policy compliance, computational cost), and each answer option is pre-mapped to one or more recommended PETs along with optional parameter suggestions.

-Scoring and Recommendations

The back-end database we have manually generated will assign scores to each PET by tallying how many times it is recommended across the user's answers. Simultaneously, we have also designed a deal-breaker system that checks whether any user answers rule out a given technology (for example: choosing "Real-time results" may veto MPC due to latency). At the end, the system ranks all PETs by their vote count (minus vetoes) and returns the top two ranked options as recommendations, accompanied by tailored configuration tips such as the k values, ε budgets, or TEE availability checks.

-Question Sequencing and Dependencies

Questions are mostly presented in a fixed order with logical dependencies. Some questions are single-select questions, while others allow multiple selections (like "What kind of data do you have?").

-How User Responses Drive Outcomes

Each response is linked to PETs and parameters via the back-end excel database we have created. Whenever a user makes a selection, the system will:

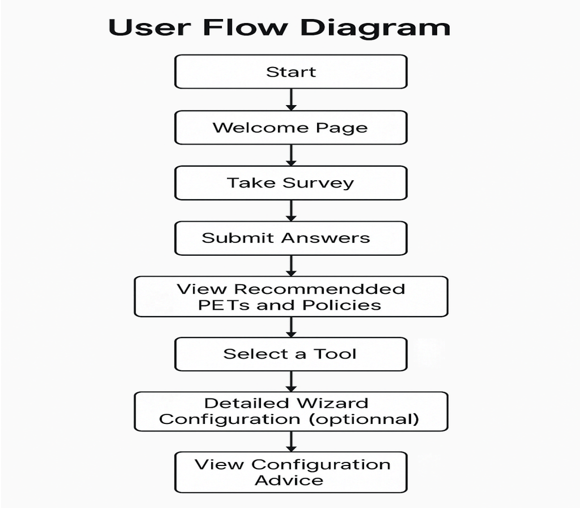
1. Tallies votes for each related PET.
2. Applies vetos to remove any unsuitable PET
3. Aggregates any suggested parameters
4. Returns a ranked list of technologies and compliance suggestions and flags any vetoed options with clear reasonings

-Challenges and Design Trade-offs

A key challenge was selecting enough questions to cover critical PET criteria without overwhelming users. We had to balance completeness with clarity, ensuring the survey remained intuitive.

Another challenge was differentiating between overlapping PETs like TEE, DP, and MPC. To address this, we implemented a weighted scoring system: each answer could contribute different weights to multiple PETs, depending on how relevant it was. This allowed us to express partial suitability and manage tie-breaks more precisely.

These weights were encoded in the Excel backend, often across multiple rows for a single answer, enabling nuanced logic. Combined with deal-breaker rules, this helped us resolve potential conflicts and generate more accurate, context-aware recommendations.


User Flow Diagram
Start
Welcome Page
Take Survey
Submit Answers
View Recommendded PETs and Policies
Select a Tool
Detailed Wizard Configuration (optionnal)
View Configuration Advice

The user begins by viewing a welcome page and answering 27 questions about their dataset, privacy preferences, and legal requirements. Based on their input, the system recommends privacy tools. The user then selects a tool and receives guidance on how to implement it.

Detailed Explanation on Questions

Each question has predefined answer options that contribute to a scoring algorithm designed to recommend suitable privacy-preserving technologies. The logic is rule-based, with each selected answer potentially contributing a +1 score to one or more PETs (privacy-enhancing technologies) and/or eliminating others through deal breaker rules.

PET Advisor also identifies relevant laws and regulations that the organization must comply with. Unlike the PET scoring system, these legal recommendations are not based on numeric weights but rather on direct rule-matching. Once the user answers yes to related legal questions, the legal compliance will appear at the end.

Type and Sensitivity of Data Involved:

Questions in this category assess dataset sensitivity and what type of data is being processed (e.g., health records, financial data, child data). For instance, if the answer indicates that the dataset contains highly sensitive health or genetic data, the system adds a +1 to **Differential Privacy**, **MPC**, and **Trusted Execution Environments (TEE)**, reflecting their strength in securing sensitive individual-level data. Questions under this category will also help the PET Advisor know which potential laws might be able to apply to them. For questions like "Does your dataset include any person's medical or health‑related information (diagnoses, treatments, lab results, prescriptions, etc.)?" If the answer is "Yes", PET Advisor will know HIPAA can apply in this dataset, and will show it in the result page under the law section.

Regulatory and Compliance Constraints:

After knowing which privacy laws might be applicable, the PET Advisor connects laws with technologies into the scoring system. For example, if a user indicates that their organization collects or processes data covered by the **General Data Protection Regulation (GDPR)**, the tool assigns a +1 to **Differential Privacy**, **Synthetic Data**, and **k-anonymity**, which are recognized for supporting GDPR's core principles of data minimization and protection by design. Similarly, if the data falls under **HIPAA** or **FERPA**, the tool will promote **Differential Privacy** or **Synthetic Data**, while simultaneously applying dealbreakers to eliminate weaker protections, such as basic anonymization methods that fail to meet the strict security and access control requirements mandated by these laws.

Data-Sharing Requirements (Internal vs. External):

Some questions in the PET Advisor assess how data is shared and who needs access to it, distinguishing between internal collaboration and external partnerships. If users indicate that data must be jointly computed by multiple untrusted entities, such as in federated analysis across organizations, **Secure Multi-Party Computation (MPC)** receives a +1 due to its strength in enabling joint computation without exposing raw data to any party. On the other hand, if data must be shared externally with partners who are not fully trusted, **Trusted Execution Environments (TEEs)** may be prioritized for their ability to isolate sensitive computations within secure hardware enclaves. In such cases, traditional techniques like **public-key cryptography** may be deprioritized, as they lack guarantees for secure runtime behavior and may not sufficiently protect data during processing.

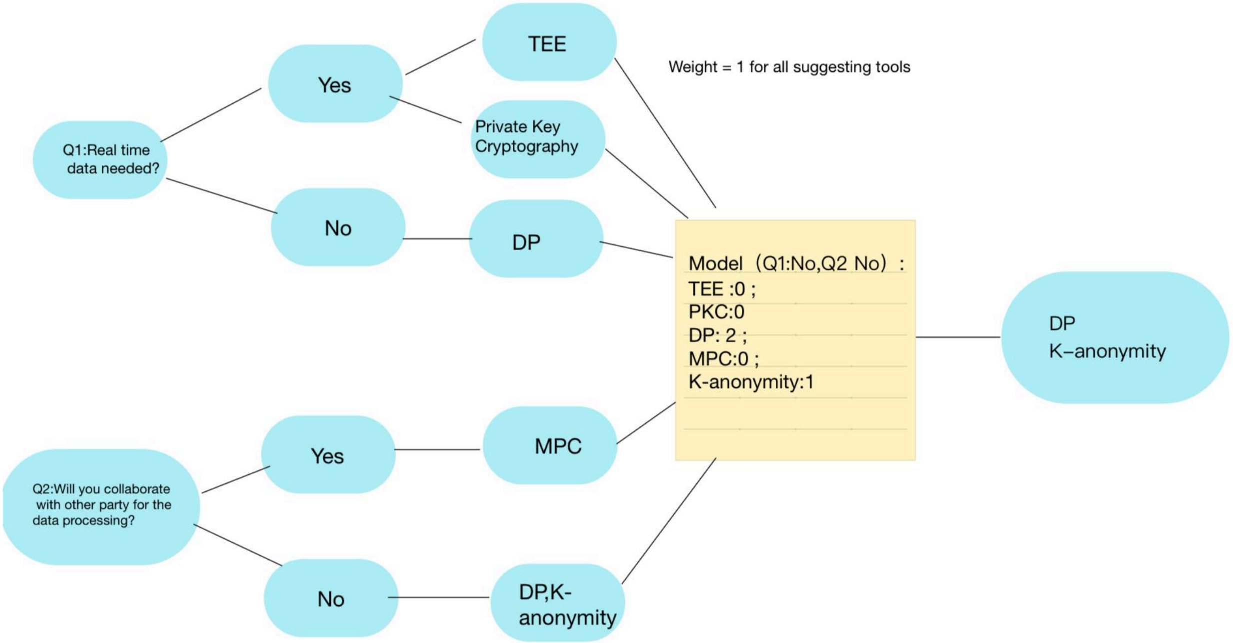
Desired Accuracy and Usability of Resulting Data:

Questions under this category evaluate the trade-off an organization is willing to make between data privacy and the accuracy of analytical results. For example, one of the questions will ask "How accurate do the results need to be?" If a user selects an option such as "exact counts (0% error)," the PET Advisor enforces deal breakers that eliminate techniques like **Differential Privacy** and **Synthetic Data**, both of which inherently introduce randomness or noise to protect privacy. In contrast, methods such as **Secure Multi-Party Computation (MPC)** and **Trusted Execution Environments (TEE)** receive a +1 because they preserve the full accuracy of the data, making them suitable for applications where precision is critical.

Computational Resources and Technical Capabilities:

The PET Advisor also accounts for the technical maturity and infrastructure of the organization when making recommendations. Techniques like **MPC** and **TEE** can require considerable setup, specialized knowledge, or access to secure hardware. As such, if a user reports limited budget or low technical expertise, the system may assign a +1 to more accessible approaches like **k-anonymity** or **Synthetic Data**, while applying a dealbreaker to exclude **MPC**. Conversely, if the organization indicates that secure enclaves are available, **TEE** receives a +1 and is prioritized as a strong candidate for enabling secure, real-time analytics.

Visualization to guide the users



Suppose the model consist with two questions, if the user answers 'No' to both, the corresponding tools—each with a weight of 1—will be suggested. After these two questions, the model will recommend Differential Privacy (DP) and k-Anonymity because they weighted the most.

Detailed explanation on the implementation subpages' algorithm

After users complete the questionnaire and receive their top two recommended privacy-preserving technologies, they can proceed to the Implementation Guidance section at the bottom of the result page. This section is interactive: users can click on either of the two suggested PETs to explore implementation recommendations, and return later to view the other. Selecting a PET opens a dedicated subpage that asks several follow-up questions tailored to the chosen technique. Each of the six supported technologies has its own algorithm-driven logic to produce actionable guidance.

For Differential Privacy, the PET Advisor uses a simplified analytical formula to compute a recommended privacy budget (ε) based on two user-supplied parameters: (1) the maximum tolerable absolute error (Δ), and (2) the expected number of queries per day (Q). Assuming a fixed delta (δ) of 1 for simplification, the algorithm assumes the use of the Laplace Mechanism, where noise is calibrated to the sensitivity of the query (typically Δ = 1) divided by ε. The Advisor rearranges this relationship to estimate ε as:

$$\varepsilon = \Delta/error$$

This value is then multiplied by the expected number of queries to determine the daily privacy budget:

Total Daily Privacy Budget = Q * ε

This gives users a practical sense of how much privacy loss accumulates with usage, and helps them balance privacy protection with analytical utility. The implementation tips then suggest concrete strategies, such as using the Laplace or Gaussian mechanism, managing budgets through composition, and applying DP at either the central or local model level, depending on organizational control over data.

Beyond Differential Privacy, the Advisor offers tailored sub-guidance for each PET. **For Secure Multi-Party Computation (MPC)**, it asks how many independent data holders are involved and whether computations require complex joins or aggregations. Based on this, it noting whether a semi-honest or malicious adversarial model is appropriate. **For Trusted Execution Environments (TEE)**, users are asked whether secure enclaves are available (e.g., Intel SGX or AWS Nitro Enclaves), and whether the system supports remote attestation. The tool then provides instructions to isolate sensitive code and data, using enclave-supported SDKs and runtime protections.

For Synthetic Data, the Advisor queries whether statistical accuracy or machine learning fidelity is more important. It recommends different generation approaches accordingly—e.g., probabilistic models (like Bayesian networks) for statistical resemblance or generative adversarial networks (GANs) for predictive modeling—along with disclosure risk mitigation techniques.

For k-Anonymity/l-Diversity, users are asked about dataset size, quasi-identifiers, and re-identification risk tolerance. The system recommends generalization and suppression strategies, depending on whether the goal is compliance or data sharing. This modular implementation wizard bridges the gap between high-level PET recommendations and real-world deployment, enabling technically proficient teams to take concrete steps toward privacy protection without requiring deep expertise in each method.

Finally, while **Cryptographic Methods** are recognized as essential in certain privacy-preserving contexts, such as secure data storage, transmission, or encrypted computation. The PET Advisor currently does not provide detailed guidance for selecting between **public-key** and **private-key encryption**. These methods often require nuanced decisions based on key management, threat models, and performance trade-offs, which typically fall within the domain of cryptography specialists.Instead, it flags cryptography as a potential consideration and encourages organizations to consult with dedicated security experts when such methods are relevant. This reflects a key limitation of the PET Advisor: while it supports practical decision-making for most PETs, highly specialized cryptographic configurations remain outside its automated scope.

One Practical Example:

Using a simulated hospital collaboration scenario. Each hospital holds patient record data, including sensitive information such as demographics, ICU admissions, comorbidities, and outcomes. The goal is to allow multiple hospitals to jointly analyze aggregated health outcomes without revealing individual patient records.

This data is not publicly released and must comply with HIPAA and institutional privacy policies. Since real patient data is involved, the system must offer strong privacy protections while preserving utility for epidemiological research and public health planning. And also with fairly low error to make data useful. By inputting answers that best fit this scenario, the model will suggest MPC and DP.

Because the data is held internally by each hospital and may be updated regularly. MPC allows hospitals to collaborate without sharing raw data, and Differential Privacy (DP) can be added to the output to further protect against inference when results are shared externally.

Technical, Policy, and Implementation Considerations

Some PETs—such as MPC and Trusted Execution Environments—introduce computational overhead or require specialized hardware. For organizations with limited infrastructure or real-time demands, deploying these tools may be impractical. Additionally, techniques like Differential Privacy require careful parameter tuning and noise management, which can strain resource-limited settings.

Ensuring compliance with laws like GDPR, HIPAA, and FOIA is not just a technical task—it requires clear documentation, consent tracking, and interpretability. Our tool flags datasets with legal implications, but implementing compliant systems still demands close collaboration between legal and technical teams.

We aimed to clarify what each PET can and cannot protect. For instance: DP defends against re-identification but doesn't protect raw inputs during computation. MPC hides inputs but doesn't prevent inference from outputs. In DP, we simplified implementation by assuming delta = 1, which may not align with all privacy risk tolerances.

Many scenarios require a hybrid approach. For example, sensitive data across institutions may need MPC for secure computation, followed by DP to protect output privacy. TEEs may provide low-latency secure computation, but should be combined with access control and encryption to mitigate hardware-level risks. We have considered doing the recommendations with hybrid methods, but there could be a lot of potential issues to think about, like whether 2 technologies would offset the effect together. And due to the intricacy and complexity of this idea, we have given up on giving hybrid recommendations but only the top 2 ranked choices.

Next Step:

After getting your results from the PET Advisor, the next step is to take those recommendations to your team—whether that's engineering, compliance, or product—and start planning how to put them into action. It's often helpful to test one of the tools on a smaller dataset first to see how it performs and what challenges might come up. If you're working with Differential Privacy, for example, you'll want to think about how to manage the privacy budget over time and truly analyze the delta value because our tool only assumes it was one. If you're considering MPC or TEEs, you'll need to make sure your systems are ready to support secure computation or hardware enclaves. To learn more and get started, you can check out trusted resources like the NIST Privacy Framework, IBM's DiffPrivLib, MP-SPDZ for MPC, or AWS Nitro Enclaves documentation. These tools and guides can help you go from planning to real implementation with confidence.

References:

Holohan, N., Braghin, S., Mac Aonghusa, P., & Levacher, K. (2019). Diffprivlib: The IBM Differential Privacy Library. *arXiv preprint arXiv:1907.02444*.

Keller, M. (2020). MP-SPDZ: A Versatile Framework for Multi-Party Computation. *IACR Cryptol. ePrint Arch.*, 2020, 521.

AWS Nitro Enclaves. Amazon Web Services.

Ping, H., Stoyanovich, J., & Howe, B. (2017). DataSynthesizer: Privacy-Preserving Synthetic Datasets. *Proceedings of the 29th International Conference on Scientific and Statistical Database Management*.

Prasser, F., Eicher, J., Spengler, H., Bild, R., & Kuhn, K. A. (2020). Flexible Data Anonymization Using ARX—Current Status and Challenges Ahead. *Software: Practice and Experience*, 50(5), 643–676.

Microsoft SEAL. Microsoft Research.