Data Privacy Scoring Rubric

Comprehensive Privacy Policy Scoring Rubric

Scoring Scale: Points assigned per criterion, with total points summing to 100.

Total Score: Sum of points across all criteria. **100 = Perfect Privacy Protection, 0 = Complete Lack of Privacy Protection.**

Criterion	Description	Scoring (Points)	Rationale &
1. Explicit Policy on AI Training (Company's Use): Allowance	Does the policy clearly state that user data *can* be used by the company to train its AI models?	**10 Points** **10:** Policy explicitly and unequivocally prohibits the use of user data for AI training. **8:** Policy is silent on AI training but has robust data minimization and purpose limitation clauses that strongly imply prohibition. **5:** Policy is vague on AI training, mentioning "improving services" or similar language that *could* be interpreted as allowing AI training, but without explicit confirmation. **2:** Policy explicitly allows the use of user data for AI training, but with stated limitations (e.g., anonymized data *only*, specific service improvement purposes, opt-out mechanisms). **0:** Policy explicitly and broadly allows the use of user data for AI training without significant limitations or user control.	Higher point prohibition. S with strong c considered g language or especially br without limita reduces poin *scope* of the presence of a controls.
2. Explicit Policy on AI Training (Company's Use): Prohibition	Does the policy clearly state that user data *cannot* be used by the company to train its AI models?	**10 Points** **10:** Policy explicitly and unequivocally prohibits the use of user data for AI training. **8:** Policy does not explicitly prohibit, but strongly implies prohibition through its stated principles and limitations on data use. **5:** Policy is silent on AI training, neither explicitly allowing nor	This criterion Criterion 1, fo presence of *p* A strong poli prohibits and training. Expl highest stand maximum po

Criterion	Description	Scoring (Points)	Rationale &
		prohibiting it. **2:** Policy does not prohibit AI training and implies its potential use under vague terms like "service improvement." **0:** Policy explicitly allows AI training, effectively negating a "prohibition" score for this criterion.	
3. Data Minimization & Purpose Limitation (General Data Collection)	To what extent does the policy demonstrate commitment to collecting only necessary data for clearly defined purposes?	**4 Points** **4:** Policy explicitly commits to data minimization, listing specific, limited categories of data collected, and clearly defining necessary purposes for each category. Data collection appears strictly proportional to the service. **3:** Policy generally adheres to data minimization principles, outlining data categories and purposes, but with minor areas of potential over-collection. **2:** Policy describes data collection, but purposes are somewhat broad or vaguely defined ("service improvement," "business purposes") raising concerns about potential data over-collection. **1:** Policy collects a wide range of data with broadly defined and potentially excessive purposes. Data collection appears disproportionate to the core service. **0:** Policy collects an extremely broad and undefined range of data with little to no justification, suggesting maximal data harvesting.	This assesses data privacy to what's trul points for po specific, limit their data co Broad, vague collection rec
4. Data Security Practices	How robust and transparent are the described data security practices?	**10 Points** **10:** Policy describes comprehensive security measures including encryption (in transit and at rest), strong access controls, regular security audits, data breach response plan, and commitment to industry best	Strong secur privacy. High that are deta commit to ro standard sec Vague or abs descriptions

Criterion	Description	Scoring (Points)	Rationale &
		practices. **8:** Policy mentions several key security measures, but may lack detail in certain areas or commitment to specific industry standards. **5:** Policy vaguely mentions "reasonable security measures" without specifics, lacking transparency and assurance. **2:** Policy provides minimal or superficial information about security practices, raising serious concerns about data protection. **0:** Policy is silent on security practices or explicitly states weak or inadequate security measures are in place.	
5. Data Retention Policy	How long is user data retained, and is the retention policy clearly defined and privacy-respecting?	**4 Points** **4:** Policy specifies short, clearly defined data retention periods based on purpose, with mechanisms for automatic deletion and user-initiated deletion requests honored promptly. **3:** Policy outlines data retention periods, but some periods may be longer than ideal or lack full clarity on specific timelines for all data types. **2:** Policy mentions data retention but is vague about specific periods, stating data is kept "as long as necessary" or similar ambiguous language. **1:** Policy describes long or indefinite data retention periods, or lacks clear justification for extended retention. **0:** Policy indicates data is retained indefinitely without justification, or is silent on data retention, suggesting potentially unlimited data storage.	Shorter, purp clearly define are more priv receive highe indefinite ret fewer points. deletion is a
6. Effectiveness of Anonymization & Pseudonymization	If the policy mentions anonymization or pseudonymization	**3 Points** **3:** Policy commits to using demonstrably robust anonymization techniques (e.g.,	This criterion anonymizatio is mentioned context of AI

Criterion	Description	Scoring (Points)	Rationale &
(if used for AI or other purposes)	, how robust and credible are the described techniques?	differential privacy, k-anonymity with specific thresholds) and provides detail on the processes used to prevent re-identification. **2:** Policy mentions anonymization/pseudonymization but provides limited detail on the specific techniques used, offering some assurance but lacking full transparency. **1:** Policy vaguely refers to "anonymized" or "pseudonymized" data without explaining the methods, raising doubts about the effectiveness and actual privacy protection. **0:** Policy claims data is anonymized but provides no details, or describes techniques that are known to be weak or easily reversible. OR Policy uses the term "anonymized" misleadingly, suggesting privacy protection without any actual anonymization process, or relies on easily reversible pseudonymization as if it were true anonymization.	sharing. Vagu unsubstantia anonymizatic protective. Lo commitment scientifically techniques fo If not applica points (3) for this dimensic
7. Specific AI Use Cases Beyond Training (Deployment)	Does the policy describe how AI is used beyond just training, and are there adequate safeguards and transparency around these applications?	**4 Points** **4:** Policy clearly outlines AI use cases (if any) beyond training and demonstrates a privacy-conscious approach, with limitations on high-risk applications (e.g., profiling, surveillance), and clear explanations of how AI impacts users. May explicitly prohibit certain privacy-invasive AI applications. **3:** Policy mentions some AI applications but lacks detail on safeguards or limitations, or focuses primarily on beneficial uses without acknowledging potential privacy risks. **2:** Policy vaguely refers to AI being used for "service improvement" or similar broad terms without specifying concrete	This goes be and looks at deployment Higher point transparent, applications, AI use. Polici AI deployme privacy-invas receive lowe deployment award maxim maximum pr dimension.

Criterion	Description	Scoring (Points)	Rationale &
		applications or privacy considerations. **1:** Policy describes AI applications that are potentially privacy-invasive (e.g., personalized advertising, content filtering) without adequate explanation of safeguards or user control. **0:** Policy promotes or implies the use of AI in highly privacy-invasive ways (e.g., facial recognition, predictive policing, automated social scoring) without any mention of ethical considerations or user protection.	
8. Data Aggregation & Inference Risks	Does the policy acknowledge and address the privacy risks associated with data aggregation and inferences drawn from user data, especially in the context of AI?	**4 Points** **4:** Policy explicitly acknowledges the risks of data aggregation and inference, and describes measures to mitigate these risks, particularly in AI applications. May commit to avoiding practices that could lead to discriminatory or privacy-invasive inferences. **3:** Policy implicitly acknowledges these risks through general privacy principles and data minimization, but doesn't explicitly address aggregation and inference as distinct concerns. **2:** Policy is silent on data aggregation and inference risks, potentially overlooking these important aspects of data privacy in the AI context. **1:** Policy may engage in practices that suggest a disregard for aggregation and inference risks (e.g., broad data sharing, combining datasets without privacy safeguards). **0:** Policy explicitly promotes or enables data aggregation and inference in ways that are likely to be privacy-invasive and discriminatory.	Even with an aggregated can reveal se Higher point aware of and these risks, e contexts. Sile these risks re

Criterion	Description	Scoring (Points)	Rationale &
9. Explicit Allowance of Third-Party Data Transmission (Scope & Purpose)	Does the policy clearly state that user data *can* be transmitted to third parties, and if so, are the scope and purpose of transmission clearly defined and limited?	**10 Points** **10:** Policy explicitly prohibits the transmission of user data to third parties except for strictly necessary service operation (e.g., payment processors, infrastructure providers), with clearly defined categories, purposes, and contractual obligations ensuring equivalent privacy protection. **8:** Policy allows limited third-party data transmission, clearly defining categories of third parties, purposes, and data types shared, emphasizing necessity, data protection agreements, and user benefit. **5:** Policy allows third-party data transmission, but categories are vague ("business partners," "affiliates") and purposes are broad ("service improvement," "marketing"), raising concerns about data misuse. **2:** Policy allows broad third-party data transmission with minimal explanation of categories, purposes, or limitations, suggesting potentially unrestricted data sharing. **0:** Policy explicitly allows unrestricted and undefined transmission of user data to any third party for any purpose, indicating a lack of control over data dissemination.	Higher point highly restric sharing. Broa unlimited sha highly detrim receive lowe necessity, an safeguards a consideratio
10. Third-Party AI Training & Human Review Permissions	If third-party transmission is allowed, does the policy explicitly prohibit third parties from using user data for their own AI training or human review?	**10 Points** **10:** Policy explicitly prohibits third parties from using transmitted user data for AI training and human review, and requires equivalent privacy standards from third parties through contractual agreements. **8:** Policy requires third parties to have privacy policies at least as protective as the company's and implies restrictions on AI training	This is condit If no third-pa award maxim third-party tr allowed, exp training and third parties maximum po permission fo third parties points.

Criterion	Description	Scoring (Points)	Rationale &
		and human review through purpose limitations and data processing agreements, though not explicitly stated. **5:** Policy is silent on whether third parties can use data for AI training or human review, creating ambiguity and potential privacy risks. **2:** Policy allows or implies that third parties can use data for their own purposes, including AI training and human review, without explicit prohibition. **0:** Policy explicitly allows third parties to use transmitted user data for AI training and human review without restrictions.	
11. Human Review of User Data (Company & Purpose)	Does the policy allow human review of user data by company employees or contractors? If so, are the purposes strictly limited, necessary, and transparent?	**10 Points** **10:** Policy explicitly prohibits human review of user data except in strictly limited and necessary circumstances (e.g., legal obligation, security incident, essential customer support), with robust oversight, minimization of data reviewed, and explicit limitations on purpose. **8:** Policy allows human review for specific, legitimate purposes (e.g., customer support, fraud prevention, system maintenance) with stated limitations on access, purpose, data reviewed, and some level of oversight. **5:** Policy allows human review for vaguely defined purposes ("service improvement," "quality assurance") without clear limitations on scope, access, or purpose, raising concerns about potential misuse. **2:** Policy allows broad human review of user data for unspecified purposes, potentially including general monitoring or analysis, with minimal limitations or oversight. **0:** Policy explicitly allows	Human revie privacy risks. prioritize mir review, limiti necessary an situations wit Broad or unc review permi points.

Criterion	Description	Scoring (Points)	Rationale &
		unrestricted and unmonitored human review of user data for any purpose, indicating a lack of respect for user privacy and potential for abuse.	
12. User Rights & Control over AI Training & Data Use (Opt-out & Granularity)	Does the policy provide users with explicit and granular rights and controls regarding the use of their data, especially concerning AI training and data sharing?	**10 Points** **10:** Policy explicitly states that user data will *not* be used for AI training (ideal) OR provides robust, easily accessible, and granular opt-out mechanisms for AI training and various types of data sharing. Offers comprehensive user rights (access, rectification, deletion, objection, data portability) that are easy to exercise. **8:** Policy provides strong general user rights (access, rectification, deletion, objection) which *could* be used to limit data use potentially including AI training and some data sharing controls, but may lack explicit opt-outs for AI training. **5:** Policy provides some user rights, but they are limited, difficult to exercise, or do not clearly extend to controlling the use of data for AI training or specific types of data sharing. Opt-out options may be buried or unclear. **2:** Policy offers minimal or unclear user rights, making it difficult or impossible for users to control how their data is used, including for AI training and data sharing. Opt-out is absent or ineffective. **0:** Policy explicitly denies users any rights to control the use of their data for AI training, data sharing, or any meaningful data rights in general, demonstrating a disregard for user autonomy.	User rights a strongest po with meaning especially ov AI training ar earning maxi Granular con exercise righ for higher pc user control

Criterion	Description	Scoring (Points)	Rationale &
13. Transparency on Data Types Used for AI (if allowed)	If the policy allows data to be used for AI training, does it clearly specify *which types* of user data are used for this purpose?	**4 Points** **4:** Policy explicitly prohibits AI training (ideal). OR if AI training is allowed, the policy transparently lists the *specific categories* of user data that may be used for AI training, allowing users to understand the scope and potential privacy implications. **3:** Policy is somewhat transparent about data types used for AI, mentioning broad categories but lacking fine-grained detail. **2:** Policy vaguely refers to "user data" being used for AI training without specifying data types, leaving users uncertain about what data is at risk. **1:** Policy is completely opaque about data types used for AI training, providing no information and hindering user understanding and risk assessment. **0:** Policy actively obscures or misrepresents the types of data used for AI training, potentially misleading users about the scope of data use.	If AI training transparency used is esser consent and earning high specification positive indic opaque lang points. If AI t award maxim maximum pr dimension.
14. Policy Change Transparency & User Notification	How transparent is the policy regarding changes, and how effectively are users notified of significant updates, especially those impacting AI or data sharing practices?	**4 Points** **4:** Policy commits to notifying users proactively and prominently of *any* changes, especially those related to AI training, data sharing, or human review, with reasonable advance notice and clear explanation of changes. Provides a version history or changelog. **3:** Policy states users will be notified of "significant" changes, but the definition of "significant" may be vague. Notification methods are described, but may not be consistently proactive or prominent. **2:** Policy mentions the possibility of changes, but notification methods are unclear or weak	Transparency changes is cr user trust and clear notifica especially th sensitive area sharing, earn of transparer notification r

Criterion	Description	Scoring (Points)	Rationale &
		(e.g., buried in website footer, no direct user notification). No commitment to proactive notification of important changes. **1:** Policy vaguely states changes can be made at any time without specific user notification commitments, eroding user trust and control. **0:** Policy explicitly reserves the right to change the policy at any time without any user notification whatsoever, indicating a lack of accountability and disregard for user awareness.	
15. Clarity & Absence of Vague/Deceptive Language	To what extent is the policy written in clear, precise, and unambiguous language, minimizing vagueness and avoiding potentially deceptive or misleading terms?	**3 Points** **3:** Policy is written in plain language, using precise terminology, defining key terms clearly, and avoiding vague or ambiguous phrases. Demonstrates a commitment to transparency and user understanding. **2:** Policy is mostly clear, with minor areas of potential ambiguity, but overall demonstrates an effort towards transparency and clarity. Minor improvements in clarity could be made. **1:** Policy contains several vague terms and phrases ("service improvement," "business purposes," "affiliates," "legitimate interests") that could be interpreted broadly, creating loopholes and potential for misuse. **0:** Policy is riddled with vague and ambiguous language, creating significant loopholes and opportunities for misuse. Key terms are undefined or broadly defined. Clarity is lacking in multiple sections. OR Policy uses actively deceptive or misleading language to obscure privacy practices, contradicts itself in	Clear, unamb essential for policy and ea points. Vague loopholes fo receives fewe language act privacy and r

Criterion	Description	Scoring (Points)	Rationale &
		different sections, or employs legalistic jargon to confuse users.	

Total Score Calculation:

Sum the points from Criterion 1 through Criterion 15. The maximum possible score is **100 points**.

Interpretation of Total Score (on 100-point scale):

- **80-100:** Excellent privacy protection. The policy strongly prioritizes user privacy in relation to AI, data handling, and transparency.
- **60-79:** Good privacy protection. The policy is generally privacy-respecting, but has room for improvement in certain areas or minor ambiguities.
- **40-59:** Moderate privacy protection. The policy offers some protections, but also allows for significant data use and sharing that could pose privacy risks. Requires careful user consideration.
- **20-39:** Weak privacy protection. The policy is permissive and allows for significant data use and sharing, including potentially for AI training, broad human review, and with limited user control. High privacy risk.
- **0-19:** Very weak to non-existent privacy protection. The policy offers minimal to no privacy protection and may actively enable privacy-invasive practices. Extremely high privacy risk.

How to Use This Rubric:

1. **Thoroughly read the privacy policy** you want to evaluate, paying close attention to sections related to data collection, use, sharing, security, and user rights.
2. **For each criterion (1-15), carefully assess the policy's language and practices** based on the descriptions provided.
3. **Assign points** for each criterion that best reflects the policy's stance, using the point scale provided within each criterion description. Be objective and justify your point assignment based on the policy text. Show the assigned points out of total points for each criterion.
4. **Provide a brief rationale** for each point assignment, explaining *why* you assigned those points and citing specific policy language where possible.
5. **Sum the points** for all 15 criteria to get the **Total Score out of 100**.
6. **Interpret the Total Score** using the score ranges provided to understand the overall level of privacy protection offered by the policy.