FORHUMANITY

BODY OF KNOWLEDGE

NECESSITY ASSESSMENT

AUTHORS:
Chris Leong & Esther Y. Chung

CONTRIBUTORS:
Kaye Grant (Template & Field Test),
Emma Day, & Alessandro De Bettin

Introduction to ForHumanity

ForHumanity's mission is to mitigate downside risks posed by AI, algorithmic, and autonomous (AAA) Systems to humans. ForHumanity endeavours to be a beacon, examining the impact of AAA Systems on jobs, society, our rights, and our freedoms. We focus on mitigating risk in the areas of ethics, bias, privacy, trust, and cybersecurity at the corporate and public policy levels, always on behalf of and for humanity.

Overview

A Necessity Assessment is an ongoing, iterative process undertaken at each stage of the AI/ML lifecycle, from Design to Decommissioning. Its purpose is to continuously assess whether or not the use of an AAA System and/or the processing of personal data is necessary to address a project's stated problem definition. Without first establishing necessity, any subsequent analysis of proportionality becomes moot. An action that is not necessary cannot be justified, regardless of how proportionate it may seem. Under the EU AI Act, which becomes fully applicable on August 2, 2026, this assessment is no longer optional for many systems. Without establishing necessity, a measure is unlawful under the Charter of Fundamental Rights (Article 52(1)) and cannot proceed to a proportionality test.

It is important to note that, within the ForHumanity audit, the Necessity Assessment is distinct from a Proportionality Study and addresses the necessity of an AAA System and/or the processing of personal data, not questions related to the balancing of human rights. The Necessity Assessment synchronises with the Proportionality Study to ensure that organisations justify the very existence of an AAA system before balancing its risks.

Much of the discourse surrounding AI is driven by a technological imperative, which can lead to the deployment of AAA Systems simply because they are technologically feasible, rather than because they are indispensable. This approach can introduce unjustified risks to individuals' privacy, rights, and freedoms. ForHumanity, therefore, mandates that a Necessity Assessment be conducted as the initial step in its Certification Schemes. This document provides guidance for performing this critical first inquiry, ensuring that organisations can demonstrate a compelling and defensible rationale for deploying an AAA System, as well as collecting and processing specific personal data.

The principle of necessity (2026 Update)

The principle of necessity, much like proportionality, is a well-established concept in law, rooted in the idea that any action that limits fundamental rights must be justified as necessary in a democratic society. The Charter of Fundamental Rights of the European Union (Article 52(1)) states that any limitation on the exercise of these rights "may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others." This principle is now governed by three primary pillars.

(1) The General Data Protection Regulation (GDPR) reinforces this principle in Article 5.1(c), which states that personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed." This concept, known as data minimisation, is a direct and practical application of necessity. The ForHumanity Necessity Assessment criteria for the Design and Development Phases have been designed to incorporate all relevant GDPR requirements, with

additional criteria to address challenges relating to decision-making in AAA Systems. The GDPR & Digital Omnibus (2026) suggests the use of Legitimate Interest as a basis for training AI models, provided that a strict necessity for the data is proven. It also introduced a specific exemption for processing sensitive data to detect and address algorithmic bias, but only if such bias correction cannot be achieved with non-personal data.

There should be a Retention/Deletion/Destruction policy in place.

(2) The EU AI Act mandates Fundamental Rights Impact Assessments (FRIA) for high-risk systems and prohibits specific practices, such as harmful behavioural manipulation, that can never be justified as "necessary". Necessity must be re-evaluated whenever a system undergoes a "substantial modification," not just at launch.

(3) The NIST AI Risk Management Framework (AI RMF), a key voluntary standard in the U.S., emphasises the need for a trustworthy AAA System lifecycle. It encourages organisations to address the ethical and societal impacts of their systems by clearly defining their purpose and scope, a process that is directly aligned with a necessity assessment. In addition, NIST AI RMF 2026 emphasises that necessity is not a one-time check but requires continuous monitoring of data flows and model drift to ensure the system remains essential throughout its lifecycle.

Additionally, new U.S. state privacy laws, such as the California Privacy Rights Act (CPRA), which went into effect on January 1, 2023, are reinforcing the principles of purpose limitation and data minimisation, requiring businesses to conduct regular risk assessments and limit the data they collect and process to what is necessary. As of January 1, 2026, California, through the California Consumer Privacy Act (CCPA), requires businesses to complete a Privacy Risk Assessment *before* any processing that presents a significant risk, which includes most automated decision-making driven by AAA Systems. Furthermore, assessments must explicitly justify retention periods, ensuring that data is deleted/destroyed as soon as its necessary purpose is fulfilled.

In 2026, the Principle of Necessity transitioned from a theoretical legal concept to a rigorous operational requirement requiring scientifically verifiable evidence. In the context of AAA Systems, necessity ensures that they are not deployed when a less intrusive implementation or even a non-technological solution would suffice. It demands a rigorous justification for the use of technology that may impact human rights, ensuring that the technology serves humanity rather than the other way around.

Who are the key stakeholders?

The **Algorithmic Risk Committee** is primarily responsible for conducting and documenting the Necessity Assessment, often in collaboration with the Data Management and Technology functions. This body is tasked with evaluating the technical and data-related aspects of the system.

The **Ethics Committee** provides crucial oversight, ensuring that the assessment aligns with the organisation's ethical principles and broader governance framework.

If a system impacts Vulnerable Populations (e.g., children, persons with disabilities, or marginalized groups), the relevant **Specialty Committee** provides

consultation and review of the Necessity Assessment. Specifically, the committee evaluates if the "least intrusive" option for the general population is also the "least intrusive" for the specific vulnerable group.

The **organisation** itself is tasked with producing, documenting, and applying the outcomes of Necessity Assessments in critical processes, such as Data Protection Impact Assessments (DPIAs) and Fundamental Rights Impact Assessments (FRIAs).

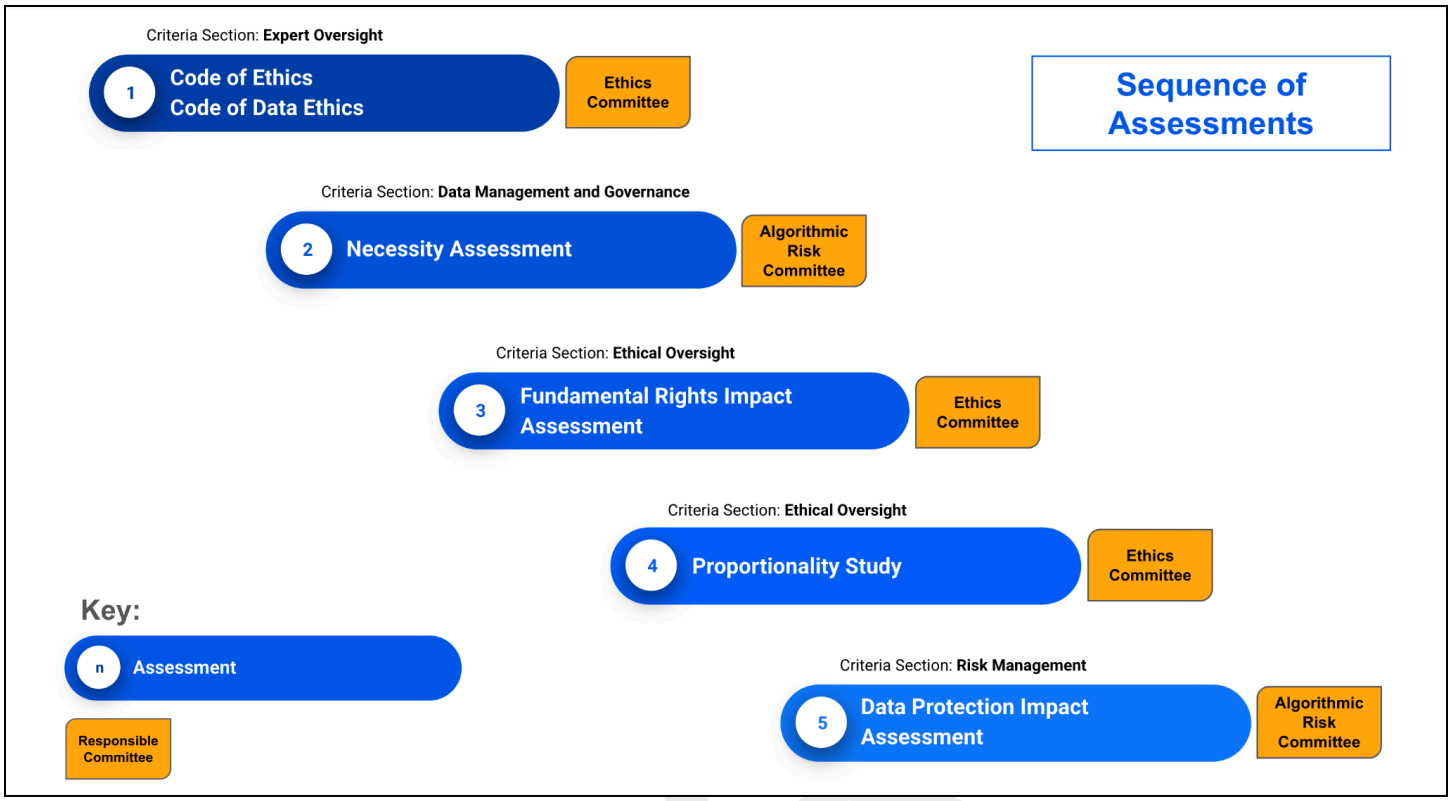
Recognising the importance of multi-stakeholder input, ForHumanity Audit Certification schemes also require engaging **Diverse Inputs and Multi-Stakeholder Feedback (DI&MSF)**, including external advisory groups and potentially impacted stakeholders. Their feedback provides crucial insights into whether the proposed system is truly necessary.

How does the Necessity Assessment integrate with other assessments?

The Necessity Assessment is a foundational assessment in the ForHumanity governance process. It must be conducted first, as its findings are a prerequisite for other, more detailed evaluations. The assessments are conducted in the following order:

- The **Code of Ethics** documents the shared moral framework of the organisation and is compiled by the Ethics Committee. The Code of Data Ethics, also compiled by the Ethics Committee, documents a set of guidelines, principles, and procedures by which data is acquired, analysed, processed, adjusted, compiled, or otherwise sold to, traded with, or shared with other entities.
- The **Necessity Assessment** examines if an AAA System is the only or best solution and if each item of Personal Datum is vital. It is conducted by the Algorithmic Risk Committee. All findings from the Necessity Assessment, including the justification for the chosen technology and the rejected alternatives, must be recorded in the Comprehensive AI Risk Evaluation (cAIRE) Report.
- The **Fundamental Rights Impact Assessment (FRIA)** examines how an AAA System and/or the processing of personal data interacts with the rights and freedoms guaranteed to the subjects of AAA Systems. It is compiled by the Ethics Committee in the Ethical Oversight section.
- The **Proportionality Study**, conducted by the Ethics Committee in the Ethical Oversight section, is only conducted if the AAA System and/or the processing of personal data passes the Necessity Assessment.
- The **Data Protection Impact Assessment (DPIA)** assesses the data protection risks in the processing of personal data. It is conducted by the Algorithmic Risk Committee in the Risk Management section. The Necessity Assessment serves as the foundation for the DPIA. The factual description generated in Step 1 of the Necessity Assessment provides the technical and operational context required for the DPIA's risk analysis.

As the sequence below shows, a Necessity Assessment provides the initial justification for the system's existence and purpose, informing and enabling the subsequent, more detailed Proportionality Study. It is a critical component of the governance structure that must be operationalised within organisations adopting and deploying AAA Systems that impact outcomes from digital services in socio-technical systems.



How do you conduct a Necessity Assessment?

A Necessity Assessment is a structured inquiry that must be conducted before any development or procurement begins. It requires a clear, rational, and evidence-based justification for the use of an AAA System. The assessment must include diverse inputs and multi-stakeholder feedback (DI&MSF), and justify the necessity of both the system itself and of the personal data it will process. This process must be documented and regularly reviewed to limit feature creep and ensure ongoing compliance throughout the AI/ML lifecycle, from Design through to Decommissioning phases:

The European Data Protection Supervisor (EDPS) Necessity Toolkit provides guidance on how a Necessity Assessment should be conducted when assessing AAA Systems and/or personal data they process. We have adapted this for AAA Systems and/or the processing of personal data:

Step 1. It requires a detailed factual description of what is being assessed (Target of Evaluation/ ToE) as necessary, along with its purpose. This should cover the AAA System and/or the scope of personal data it will process.

Step 2. It requires the identification of any limitation on the rights to the protection of personal data or respect for private life, impacting the right to privacy and possibly other rights, by the use of the AAA System and/or the processing of personal data.

Step 3. It assesses the necessity of the AAA System and/or its processing of personal data in consideration of the purpose/objective of that AAA System and/or processing of personal data, which

must comply with the relevant legal frameworks and protect the rights and freedoms of others (legitimacy).

Step 4. When performing the Necessity Assessment, it provides guidance on the specific aspects to address, in particular, that the measures considered in the AAA System and/or processing of personal data should be effective and the least intrusive.

If the assessment of any of the elements detailed in Steps 2 to 4 leads to the conclusion that AAA System and/or the processing of personal data might not comply with the requirement of necessity, then the AAA System and/or the processing of personal data should either not be proposed, or should be reconsidered in line with the results of the analysis.

We then apply Steps 1 to 4 in each phase of the AAA System lifecycle: from the Design phase through to the Decommission phase, as outlined below:

Phase	Step 1: Factual Description	Step 2: Identification of Fundamental Rights and Freedoms	Step 3: Definition of Objectives	Step 4: Effective and Least Intrusive Option
Design	• Provide a detailed factual description of the ToE, including the data categories, the actors involved, and the intended processing operations.	• Identify any limitations on fundamental rights posed by the proposed AAA system and processing of personal data.	• Document the specific, legitimate, and lawful purpose that the AAA system and/or processing of personal data is intended to achieve, in reference to the specific and relevant legal frameworks.	• Determine specific measures in the ToE that are effective and least intrusive. • Demonstrate that the system is indispensable because no other less intrusive means could achieve the same result with comparable effectiveness. • Document all rejected alternatives and necessity justifications with objective evidence in the Comprehensive AI Risk Evaluation (cAIRE) report.
Development	• Review alignment of scope, context, nature & purpose of ToE against the detailed factual description.	• Verify that the limitation does not empty the right of its basic content (respect the "essence" of the right).	• Integrate scientifically verifiable evidence that supports the existence of the problem that the system aims to solve.	• Default to the simplest possible technological implementation. Mere convenience or cost-effectiveness is not a sufficient justification for more complex solutions.
Deployment	• Review alignment of scope, context, nature & purpose of ToE against the detailed factual description..	• Assess Data Quality and Information Quality to ensure that the data is fit for purpose and that any inherent biases are understood. Poor-quality data can render the AAA system unnecessary. • Where it was necessary to utilise an AAA System that has inherent risk of negative outcome(s) and/or a dataset that	• Conduct a data minimisation test and confirm that each item is vital to the objective and strictly necessary for the AAA system to function. • Re-assess the necessity of respective component(s) of the AAA System and/or personal data processed to ensure compliance with the Relevant Legal Frameworks.	• Verify that the AAA system and/or processing of personal data, through comprehensive impact analysis, testing, and validation, does not ethically impact humans and that all security risks, such as adversarial attacks, are mitigated.

Phase	Step 1: Factual Description	Step 2: Identification of Fundamental Rights and Freedoms	Step 3: Definition of Objectives	Step 4: Effective and Least Intrusive Option
		could be deemed unethical but allowed under the exemptions of respective regulations within applicable jurisdictions, assess and provide the corresponding Automated Decision-making Explainability Statement	• Confirm that the business insights or outputs are not in conflict with the Code of Ethics or Code of Data Ethics.	
Operation	• Conduct regular reviews to ensure that the AAA's system's scope, context, nature, and purpose continue to align with the detailed factual description.	• Ensure that individuals are notified about the processing as soon as it no longer jeopardises the purpose (e.g., following secret surveillance).	• Implement continuous monitoring of the AAA system's performance through automated logging and feedback loops for human review on demand. • Enable a human to intervene in the operation of the AAA System in a timely manner to prevent harm or hazard from occurring. • Implement monitoring for model, data, or concept drift. If effectiveness drops below a rejected alternative, necessity must be re-evaluated.	• Conduct risk and impact analysis as well as implement controls (e.g., kill-switches and/or alert notifications) to ensure that the system operates within its designated scope and purpose. • Establish objective criteria restricting the number of persons authorised to access data to the strict minimum based on operational necessity.
Decommission	• Archive all components of the ToE in a centralised repository to ensure reproducibility and future reference.	• Assess if any residual data remains that could lead to post-decommissioning discrimination or privacy impacts.	• Verify that the decommissioning process fulfils the organisational objective or responsible lifecycle management.	• Reference the Retention/Deletion/Destruction policy. The duration of retention should be based on how long the data effectively contributes to the purpose.

References

Requirements from the ICO :
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how7

The European Data Protection Supervisor (EDPS) Necessity Toolkit :
https://www.edps.europa.eu/sites/default/files/publication/17-04-11_necessity_toolkit_en_0.pdf

Charter of Fundamental Rights (Article 52(1)) :
https://fra.europa.eu/en/eu-charter/article/52-scope-and-interpretation-rights-and-principles

General Data Protection Regulation (GDPR) :
https://gdpr.eu/

NIST AI Risk Management Framework (AI RMF) : https://www.nist.gov/itl/ai-risk-management-framework

California Consumer Privacy Act (CCPA) :
https://oag.ca.gov/privacy/ccpa

NECESSITY ASSESSMENT

ForHumanity Independent Audit of AI Systems

AAA System Name	
Organization	
Assessment Version	
Date of Assessment	
Current Lifecycle Phase	
Assessment Lead (ARC)	
Ethics Committee Rep(s)	
Specialty Committee Rep(s)	
Code of Ethics Reference	
Code of Data Ethics Reference	

HOW TO USE THIS DOCUMENT: This document is organized around the Necessity Assessment BoK's core framework: 4 Steps applied across 5 lifecycle phases. ForHumanity criteria requirements traceable via the Appendix. Complete the 4 steps for each lifecycle phase starting from Design. The assessment must be re-conducted when the system undergoes a material change to Scope, Context, Nature, or Purpose (SNCP).

Prerequisites (Must Exist Before Assessment)

[ ] Code of Ethics
[ ] Code of Data Ethics
[ ] Ethics Committee consultation scheduled/completed
[ ] SNCP (Scope, Nature, Context, Purpose) documented
[ ] Vulnerable Populations identified - Specialty Committee formed (if applicable)
[ ] DI&MSF pool established and integrated

VULNERABLE POPULATIONS NOTICE: Per the BoK, the "least intrusive" option must be evaluated for each specific vulnerable group at every step of every lifecycle phase.

PART A: ASSESSMENT CONTEXT AND SCOPE

A.1 System Overview

Provide the SNCP-level description of the AAA System.

AAA System Name	
System Description	
Primary Purpose	
Legal Basis for System	
Current Lifecycle Phase	

A.2 Assessment Type

Does the system collect, process, or use Personal Data?	[ ] Yes [ ] No
Personal Data NA required? (Mandatory if Yes above)	[ ] Yes — MANDATORY
Non-Personal Data NA? (Recommended)	[ ] Yes

A.3 Stakeholders Considered

Stakeholder Category	Identified Stakeholders
Direct Stakeholders	
Indirect Stakeholders	
Domain Experts	
Vulnerable Populations	
Protected Categories	
Intersectionalities	

A.4 Vulnerable Populations Assessment

Does this system impact Vulnerable Populations?	[ ] Yes [ ] No
Specialty Committee formed?	[ ] Yes [ ] No [ ] N/A
Specialty Committee members	
Disability Inclusion & Accessibility Committee consulted?	[ ] Yes [ ] No [ ] N/A

Identified Vulnerable Populations for This System

Vulnerable Group	How They Are Affected

A.5 Ethics Committee & DI&MSF Consultation

[ ] Ethics Committee consultation conducted

Date(s) of Consultation:

Members Consulted:

[ ] Guided by Code of Ethics

[ ] Guided by Code of Data Ethics

[ ] DI&MSF (Diverse Input & Multi-Stakeholder Feedback) integrated

[ ] DI&MSF pool meets diversity sufficiency requirements

PART B: THE NECESSITY ASSESSMENT

DESIGN PHASE

Step 1: Factual Description (Design)

Provide a detailed factual description of the ToE, including data categories, actors involved, and intended processing operations.

Target of Evaluation (ToE):

Data Inventory (Consolidated)

P=Personal; NP=Non-Personal; VP Impact=Does this datum specifically affect Vulnerable Populations? Vital=Is this datum vital to the objective? Nec=Is this datum necessary?

Datum	Type P/NP	Source	Collection	Purpose	Vital?	Nec?	VP Impact?	Justification

Actors Involved

Actor / Role	Involvement with Data	Access Level

Step 2: Identification of Limitations on Rights (Design)

Identify any limitations on fundamental rights posed by the proposed AAA system and processing of personal data. Verify that the limitations do not empty the right of its basic content (respect the essence of the right).

Rights checklist (EU Charter of Fundamental Rights — applicable by reference for high-risk systems; US equivalents apply for US deployments):

[ ] Article 7 — Respect for Private and Family Life (Privacy)
[ ] Article 8 — Protection of Personal Data
[ ] Article 21 — Non-Discrimination
[ ] Article 47 — Right to an Effective Remedy and Fair Trial
[ ] Article 1 — Human Dignity

[ ] Article 6 — Right to Liberty and Security
[ ] Article 20 — Equality Before the Law
[ ] Article 38 — Consumer Protection
[ ] Right to Essential Services / Equitable Access to Public Goods (US constitutional and statutory equivalents)

Right / Freedom	How System May Limit It	Applicable Law(s)	VP Disproportionate?	Justified?

Specialty Committee / VP Review:

Step 3: The Necessity Test (Design)

Purpose & Objective

Description.

Is the AAA System the only or best solution?	[ ] Only [ ] Best [ ] No
Is each Personal Datum vital to the objective?	[ ] All vital [ ] Partially [ ] N/A

Justification:

Alternatives Considered and Rejected

Alternative	Why Rejected	Evidence

All rejected alternatives must be documented with objective evidence in the cAIRE Report.

Step 4: Effective and Least Intrusive Option (Design)

Description

Vulnerable Group	Least Intrusive for This Group?	If No, What Adjustment?

Specialty Committee sign-off date:

Design Phase Conclusion

[ ] PASS — System passes the necessity test at Design phase
[ ] FAIL — System fails; must be reconsidered before proceeding
[ ] CONDITIONAL — Passes with mitigations (documented below)

Mitigations / Conditions:

DEVELOPMENT PHASE

Step 1: Factual Description (Development)

Review alignment of scope, context, nature & purpose of ToE against the detailed factual description from Design.

Does the system as built align with the Design description?	[ ] Yes [ ] No

Deviations from Design:

Step 2: Identification of Limitations (Development)

Verify that the limitation does not empty the right of its basic content — respect the 'essence' of the right.

Does the implementation respect the essence of identified rights?	[ ] Yes (conditional) [ ] No
Has the ARC/Ethics Committee verified this for Vulnerable Populations?	[ ] Yes [ ] No

Evidence / Explanation:

Step 3: Necessity Test (Development)

Integrate scientifically verifiable evidence that supports the existence of the problem the system aims to solve.

Scientifically Verifiable Evidence:

Step 4: Effective and Least Intrusive (Development)

Default to the simplest possible technological implementation. Mere convenience or cost-effectiveness is not sufficient justification for more complex solutions.

Is this the simplest possible technological implementation?	[ ] Yes [ ] No
Specialty Committee / ARC confirmation: chosen implementation also least intrusive for each VP group?	[ ] Yes [ ] No

Justification for technology choice:

Development Phase Conclusion

[ ] PASS
[ ] FAIL
[ ] CONDITIONAL

Mitigations / Conditions:

DEPLOYMENT PHASE

Step 1: Factual Description (Deployment)

Review SNCP alignment. Assess Data Quality and Information Quality.

[ ] SNCP still aligned with factual description
[ ] Data Quality assessed — data is fit for purpose (Poor-quality data can render the AAA system unnecessary)
[ ] Inherent biases understood and documented
[ ] Where a dataset is deemed unethical but allowed under the exemptions of respective regulations within applicable jurisdictions, was the corresponding Automated Decision-making Explainability Statement provided and assessed?

Data quality findings:

Step 2: Identification of Limitations (Deployment)

Where it was necessary to utilise a system with inherent risk of negative outcomes, provide the Explainability Statement.

[ ] Explainability Statement provided

Do biases disproportionately affect Vulnerable Populations?	[ ] Yes [ ] No [] Pending

Specialty Committee / ARC assessment of VP impact at deployment:

Step 3: Necessity Test (Deployment)

[ ] Data minimisation test conducted
[ ] Component necessity re-assessed
[ ] Outputs not in conflict with Code of Ethics
[ ] Outputs not in conflict with Code of Data Ethics

Findings:

Step 4: Effective and Least Intrusive (Deployment)

[ ] Impact analysis completed
[ ] Testing and validation completed
[ ] Security risks mitigated

VP-specific testing:

Evidence:

Deployment Phase Conclusion

[ ] PASS
[ ] FAIL
[ ] CONDITIONAL — Cannot proceed to deployment until all PENDING items above are resolved

Mitigations / Conditions:

OPERATION PHASE

Step 1: Factual Description (Operation)

Review frequency: Annual minimum; also triggered by material changes to SNCP, significant economic/demographic shifts in service areas, or detection of model/data drift.

Last review date:

[ ] SNCP still aligned

Step 2: Identification of Limitations (Operation)

Ensure individuals are notified about processing.

[ ] Individuals notified about processing

Notification mechanism:

Are Vulnerable Populations receiving accessible notifications?	[ ] Yes [ ] No

Step 3: Necessity Test (Operation)

[ ] Continuous monitoring implemented (automated logging, feedback loops)

[ ] Human intervention capability enabled

[ ] Drift monitoring in place (model / data / concept)

Drift findings:

VP disproportionately affected by any detected drift?	[ ] Yes [ ] No [] Not yet assessed

Step 4: Effective and Least Intrusive (Operation)

[ ] Kill-switch / alert notifications implemented

[ ] Data access restricted to operational minimum

[ ] Was there objective criteria restricting the number of persons authorised to access data to the strict minimum based on operational necessity?

ARC periodic review of VP impact during operations?	[ ] Yes [ ] To be established

Operation Phase Conclusion

[ ] PASS
[ ] FAIL
[ ] CONDITIONAL

DECOMMISSION PHASE

Step 1: Factual Description (Decommission)

[ ] All ToE components archived in centralised repository
Repository location: To be specified

Step 2: Identification of Limitations (Decommission)

[ ] Residual data assessed To be completed at decommissioning

Could residual data disproportionately harm Vulnerable Populations?	[ ] Yes [ ] No [ ] To be assessed at decommission

Findings: To be completed at decommissioning.

Step 3: Necessity Test (Decommission)

[ ] Decommissioning fulfils responsible lifecycle management objective

Step 4: Effective and Least Intrusive (Decommission)

[ ] Retention/Deletion/Destruction policy (including notification requirements) implemented

Retention period and justification:

Retention/Deletion/Destruction policy considers VP-specific data sensitivity?	[ ] Yes [ ] No

Non-Deprivation at Decommission:

PART C: CRITERIA COMPLIANCE — 9 MANDATORY ELEMENTS (A–I)

ForHumanity criteria requirements for Personal Data NA. Cross-reference with Part B where applicable.

Elem	Requirement	Description	Status	Part B Ref
A	Culture & Procedures	Regular assessment of 8 aspects (components, architectural input, databases, technical infrastructure, energy/resource, environmental impacts, security protocols, storage) for potential omission		Design Step 1 (Data Inventory); Operation Step 1 (SNCP review)
B	Problem Statement	Document the problem statement justifying the system and personal data collection — chronically delinquent accounts, limited assistance program reach, hidden financial stress, costly/inconsistent manual review		Design Step 3 (Necessity Test)
C	Precise Data Specs	Precise specifications of personal data required — see Data Inventory (Part B Design Step 1): payment history, outstanding balances, bill amounts, usage, address, household income		Design Step 1 (Data Inventory)
D	Data Handling	Process to identify and archive/delete/destroy unnecessary personal data		Decommission Step 4
E	Risk Controls	Risk controls, treatments, mitigations for unnecessary personal data, with traceability — bias monitoring, quarterly ARC review, override logging, kill-switch protocol		Design Step 4; Operation Steps 3 & 4
F	Review / Feature Creep	Regular review schedule; assess changes to limit feature creep — annual review minimum; material change triggers documented in Part E		Part E: Keeping Current
G	Technical Design	Technical design decisions ensuring data minimization — three-category data structure; no social media/biometric data; structured data only; minimum fields confirmed in Data Inventory		Design Step 4 (Least Intrusive)
H	Simplest Implementation	Default to simplest possible technological implementation — supervised ML regression on structured data; non-generative; non-biometric; human-in-the-loop maintained		Development Step 4
I	Auditable Lifecycle	Lifecycle designed to be auditable		All phases; Part D outputs

PART D: HOW THIS NA FEEDS OTHER DOCUMENTS

Examples

Document	Required?	Status	Reference	Criteria Ref
Business Rationale Report	If applicable		To be completed — causal hypothesis, construct validity, feature relevance; RCT evidence to be incorporated	CO-GL-PR-BR-AC-2602-001
Algorithmic Risk Assessment / cAIRE Report	Required		NA findings (necessity, alternatives, VP risks, data inventory) to be incorporated; cAIRE Report template available	CO-GL-PR-RM-AC-2602-022
Risk Log	Required		All risks identified in this NA (bias risk, proxy discrimination, VP specific risks) to be entered in Risk Log	CO-GL-PR-RM-AC-2602-002
DPIA (as Element P)	Required (Personal Data)		NA foundational description (Step 1) provides technical and operational context for DPIA risk analysis	CO-GL-PR-RM-AC-2602-006
Data Protection Policy	If applicable		CCPA compliance documented in DI&MSF Handbook; full Data Protection Policy to reference this NA	CO-GL-PR-DM-DL-2602-001
Proportionality Study	If NA passes		Step 4 findings (least intrusive analysis, VP tensions) feed into Proportionality Study (Ethics Committee); conditional pass enables this	CO-GL-PR-ET-EC-2602-020
FRIA	If applicable		FRIA document exists	CO-GL-PR-ET-EC-2602-020
Explainability+ Statement	Required pre-deployment		NA necessity justification and data inventory inform contents of Explainability+ Statement	CO-GL-PR-EX-EC-2602-003
System Design Report	If applicable		Design phase findings inform System Design Report	CO-GL-PR-DC-AC-2602-001
System Development Lifecycle Log	If applicable		RCT validation and development decisions to be logged	CO-GL-PR-DC-AC-2602-001
Decommissioning / Change Mgmt Plan	If applicable		Decommission phase findings inform plan;	CO-GL-PR-RC-AC-2602-005

PART E: KEEPING CURRENT

Update Triggers

#	Trigger
1	Material change to the AAA System's Scope, Nature, Context, or Purpose (SNCP) — including new data sources, new use cases, significant model architecture changes, new deployment jurisdictions
2	Detection of model drift, data drift, or concept drift that causes the system's effectiveness to approach or fall below a previously rejected alternative — triggers necessity re-evaluation
3	Significant regulatory or legal changes in any deployment jurisdiction affecting legal basis, data minimisation requirements, or algorithmic decision-making obligations (e.g., new state AI laws, CCPA updates, federal algorithmic accountability legislation)
4	Detection of disparate impact or bias patterns in quarterly ARC review that disproportionately affect Vulnerable Populations or protected categories — triggers VP-specific necessity re-assessment
5	Emergency triggers: pandemic, economic crash, natural disaster, or significant economic disruption in service areas

Review Schedule

Review Frequency: Annual minimum review (and at each material change trigger above); quarterly ARC review of model performance, bias indicators, and VP impact; monthly monitoring of automated logging and feedback loops.

Responsible Party: Algorithmic Risk Committee (ARC) — primary; Ethics Committee — oversight and sign-off on annual review; Annual External Review

Review Procedure: (1) ARC reviews SNCP alignment and data inventory currency; (2) bias/fairness metrics reviewed against thresholds; (3) VP impact assessed; (4) Ethics Committee presented with findings; (5) any conditional items from prior review resolved or escalated; (6) version control updated; (7) if material changes detected, Steps 1–4 re-run for affected lifecycle phase(s).

Version Control

Version	Date	Changes	Updated By	Approved By

CERTIFICATION

By signing below, the ARC, Ethics Committee, and Specialty Committee certify this Necessity Assessment has been conducted in accordance with ForHumanity criteria, is guided by the Code of Ethics and Code of Data Ethics, considers Vulnerable Populations throughout, and will be kept current throughout the system lifecycle.

Algorithmic Risk Committee Lead	Name: _____ Signature: _____	Date: _____
Ethics Committee Lead	Name: _____ Signature: _____	Date: _____
Top Management Representative	Name: _____ Signature: _____	Date: _____

Note:

APPENDIX: TRACEABILITY MATRIX

Maps this document to ForHumanity criteria. Include criteria reference IDs for direct traceability to the scheme.

Section	What It Covers	ForHumanity BoK / Criteria	FH Unique Identifier
Part A — Context	System ID, legal basis, stakeholders, VP assessment, EC consultation	NA Definition; Data Mgmt & Governance	CO-GL-PR-DM-AC-2602-004; CO-GL-PR-RM-AC-2602-006 (CT-03.01)
Part A.4 — Vulnerable Populations	VP identification, ARC/EC formation, DPIA VP assessment	BoK Stakeholders; Specialty Committee; DPIA VP assessment	CO-GL-PR-RM-AC-2602-006 (CT-01.05); CO-GL-PR-BM-DL-2602-003
Part B — Design	Factual description, rights ID, necessity test, least intrusive, VP test	BoK Steps 1–4 (Design); Data Mgmt & Governance	CO-GL-PR-DM-AC-2602-004; CO-GL-PR-DM-AC-2602-003
Part B — Development	Alignment, essence of rights, evidence, simplest tech, VP confirmation	BoK Steps 1–4 (Development)	CO-GL-PR-DM-AC-2602-004
Part B — Deployment	Data quality, explainability, minimisation, impact analysis, VP testing	BoK Steps 1–4 (Deployment)	CO-GL-PR-DM-AC-2602-004; CO-GL-PR-RM-AC-2602-006 (CT-03.01)
Part B — Operation	Review, notification, drift monitoring, access controls, VP drift impact	BoK Steps 1–4 (Operation)	CO-GL-PR-DM-AC-2602-004; CO-GL-PR-DM-AC-2602-006
Part B — Decommission	Archive, residual data, retention policy, VP data sensitivity	BoK Steps 1–4 (Decommission)	CO-GL-PR-RC-AC-2602-005 (CT-03.02.02)
Part B — Data Inventory	Each datum assessed vital/necessary + VP impact	NA Definition; Data Mgmt & Governance	CO-GL-PR-DM-AC-2602-004; CO-GL-PR-DM-AC-2602-005
Part C — Elements A–I	9 mandatory elements for Personal Data NA	Data Mgmt & Governance (A–I)	CO-GL-PR-DM-AC-2602-004
Part D — Business Rationale	Causal Hypothesis, Feature Relevance, Construct Validity	Business Rationale	CO-GL-PR-BR-AC-2602-001; CO-GL-PR-BR-AC-2602-003
Part D — DPIA	NA included as element of DPIA	Risk Management (DPIA)	CO-GL-PR-RM-AC-2602-006 (CT-03.01)
Part D — Ethical Oversight	EC assesses test changes against NA	Ethical Oversight	CO-GL-PR-ET-EC-2602-020
Part D — Bias Mitigation	Sensitive Data collection per NA for VP/bias	Bias Mitigation	CO-GL-PR-BM-DL-2602-003 (CT-04.02)
Part D — Explainability+	NA informs Explainability+ Statement contents	Explainability	CO-GL-PR-EX-EC-2602-003

Part E — Keeping Current	Update triggers, review schedule, version control	Data Mgmt & Governance (keep current)	CO-GL-PR-DM-AC-2602-004
Expert Oversight	NA referenced in training requirements	Expert Oversight	CO-GL-PR-EO-TM-2602-002 (CT-01.03)

FORHUMANITY