APPENDIX 1

POSTCOVIDATA IMPACT ASSESSMENT

[Project Owner]
[Project Name]
PostCoviData Impact Assessment ("PIA")

<Day> <Month> <Year>

1. PROJECT SUMMARY

(Describe the Pandemic Tech Solution, the dataset and the context)

In this document, "**Pandemic Tech Solution**" means a software solution, device or product developed or deployed by the Project Owner that integrates data-driven functionalities.

Describe the project and what it intends to achieve by addressing the following key points:

- *Describe the Pandemic Tech Solution as a whole, including a functional description/overview and the datasets.*
- *What does the Pandemic Tech Solution seek to achieve?*
- *What is the political and social context in which the Pandemic Tech Solution would be deployed or used?*
- *Does the Pandemic Tech Solution raise issues of specific ethical concern that should be explored prior to proceeding?*
- *Where does the PIA sit within the project timeline? Is it intended to evolve?*
- *What is the Project Owner trying to achieve with the Pandemic Tech Solution?*
- *Is the Pandemic Tech Solution a one-off initiative or part of ongoing business development?*

Project summary

[NOTE: Is this Pandemic Tech Solution an expansion of a previous activity? If yes, determine whether a previous assessment has been done. If a previous assessment has been done, what has changed in this data activity and why (refer to previous assessment)?*]*

Dataflow chart

Governance structure

2. KEY FACTORS FOR CONDUCTING A PIA

The first step in conducting a supplemental Pandemic Tech Solution Impact Assessment should be an evaluation of why that specific Pandemic Tech Solution requires such a PIA, with regard to any Risk Impact Assessment already conducted.

To conduct this first step, the Project Owner should define clearly the scope and goals of the Pandemic Tech Solution and the characteristics of the envisioned Pandemic Tech Solution. At this stage, many elements need to be considered, but the analysis need not be as thorough as at the main assessment. Important criteria to consider are listed in the Table below (note that this list is non-exhaustive and should be adapted to the specific context of the Project Owner). It should be noted that this PIA will need to be continuously adjusted as the scientific community confirms the pandemic's characteristics. The present PIA will also need to be adjusted based on evolving knowledge about the impact of any tech solutions on individuals and societies.

At this preliminary stage as well as during the main risk assessment, risks factors should be evaluated based on low to high risk scale (low, medium, high). A holistic and contextual approach is recommended. Such an approach should consider the factors in relation to one another. For instance, a Pandemic Tech Solution deployed strictly internally to support certain decision-making processes might be said to be, in general, less risky than a citizen-facing system. However, an internal Pandemic Tech Solution used to evaluate or monitor employees might trigger certain labour laws obligations and in consequence be riskier than certain citizen-facing systems.

Factors Justifying Need For Impact Assessment	Risk Rating (Low, Medium, High)	Commentary
1. What is the context in which the Pandemic Tech Solution will be used or deployed? Would this use be citizen-facing?		
2. Does the country have data protection laws or regulation? How does it fare on rule of law? Is the Pandemic Tech Solution deployed in an exception legal context (state of emergency)?		
3. Will the Pandemic Tech Solution be used across legal jurisdiction borders (whether they be across federal states or country borders)?		
4. Who will be the categories of persons involved in the Pandemic Tech Solution?		
5. What is the type and origin of the data that will be used to train the Pandemic Tech Solution? Will, in the context of an AI solution, the training data include personal information? What is the level of sensitivity of the data? Who are the data subjects?		
6. What kind of decisions will the Pandemic Tech Solution be making? What rights and interests will be at stake? Are those rights fundamental or human rights?		
7. What is the expected degree of autonomy of the Pandemic Tech Solution? Will, for instance, human operators or decision-makers have oversight on individual AI decisions, if any? How frequently will oversight occur? What measures will be made to avoid automation bias or anchoring to the Pandemic Tech Solution?		
8. What are the technical characteristics of the Pandemic Tech Solution that could influence the explainability and auditability of the algorithm? Can the Pandemic Tech Solution be explained?		
9. What will be the Project Owner's degree of control and responsibility over the finalized Pandemic Tech Solution? Who are the expected contributing third parties?		
Synthesis (is this supplemental PIA required/useful and key points leading to this conclusion):		

3. MAIN ASSESSMENT

Each row in the following table summarises the key requirements of responsible Pandemic Tech Solution principles and outlines some key questions or considerations you should address. See the checklists provided in the attached **Appendix 1** for assistance in what documents should be consulted and what information should be included in filling out the following table.

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
Principle #1: Ethical Purpose and Societal Benefit *Project Owners that develop, deploy or use Pandemic Tech Solution and any national laws that regulate such use should require the purposes of such implementation to be identified and ensure that such purposes are consistent with the overall ethical purposes of beneficence and non-maleficence, as well as the other principles.*				
Overview of the Principle • The Project Owner should review the objectives of the Pandemic Tech Solution, e.g. ensuring consistency in decision-making, improving operational efficiency and reducing costs, or introducing new product features to increase citizen choice. The Project Owner should then weigh them against the risks of using the Pandemic Tech Solution in the Project Owner's decision-making. • The Project Owner should gather the key stakeholders required for the discussion/decision, including: – Internal stakeholders (project manager, chief scientist, officer, board member, employees, civil society etc.) – External (developer, external data provider, research partner, distributor, etc.) – End user (citizen, service user, etc.) – Government (public institution, regulatory agency, etc.) – Members of vulnerable groups requiring special care (children, disabled persons, people with little technological literacy, etc.) In determining the level of human oversight, the Project Owner should consider the impact of the decisions of the Pandemic Tech Solution on the individual, group of individuals and on society in general. On that basis, the Project Owners should identify the required level of human involvement in the decision-making of the Pandemic Tech Solution.				
PART I – GENERAL ASSESSMENT APPLYING TO ALL TECH SOLUTIONS				
1. What laws apply to the collection, analysis and use(s) of data?				
2. Are there other legal, cross-border, policy, contractual, industry or other obligations linked to the collection, analysis and use(s) of data?				
3. May the Pandemic Tech Solution be deemed as medical device or any other qualification that could entail application of other regulation (e.g. medical secrecy) that could modify its ethical perception?				
4. Does the Pandemic Tech Solution comply with the values, standard and policies of the Project Owner?				
5. What are the potential reputational and material risks for the Project Owner?				
6. Will the deployment or use of the Pandemic Tech Solution affect the autonomy of the affected stakeholders?				
7. Consider appropriate safeguards to promote the informed human agency, autonomy and dignity of employees and to avoid inappropriate or destructive impacts on the emotional or psychological health of employees (monotony of tasks, excessive surveillance, gaming of behavior, continuous exposure to horrific content).				
8. Consider any other appropriate safeguards that should be assessed, as time-limit, automatic deletion.				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
PART II – SPECIFIC ASSESSMENT APPLYING TO AI AND MACHINE-LEARNING BASED SOLUTIONS				
9. Consider whether it is achievable from a technological perspective to ensure that all possible occurrences should be pre-decided within the Pandemic Tech Solution to ensure consistent behavior. If this is not the case, consider how the outcomes (aka machine behaviours) will be monitored and fed back into the governance and oversight framework.				

Principle synthesis

- *Is the Pandemic Tech Solution compatible with human agency, human autonomy and the respect for fundamental human rights?*
- *Does the Pandemic Tech Solution comply with the ethical purposes of beneficence and non-maleficence?*
- *What are the risks of harm to persons and their rights of this Pandemic Tech Solution?*
  - Should notably be considered as a risk factor the possibility given to individuals to decline to install the solution and to uninstall it/remove it from devices.
  - Should also be considered the proportionality of the collection of device data regarding the aims of the solution.
  - Should be considered as well whether the Project Owner has implemented effective measures to ensure human control and oversight on the automated decision-making process of the solution, if any.
  - Should also be investigated the broader impact that use of the solution may have on stakeholders other than the end-user.

Principle #2: Accountability

Project Owners that develop, deploy or use Pandemic Tech Solution and any national laws that regulate such use shall respect and adopt the seven principles developed in the framework (or other analogous accountability principles). In all instances, humans should remain accountable for the acts and omissions of data-driven systems.

Overview of the Principle — The Project Owner should ensure at all times that it remains accountable for the ethical and responsible deployment of Pandemic Tech Solutions that the Project Owner deploys, including by means of “human-in-the-loop” or “human-over-the-loop” deployment.

PART I – GENERAL ASSESSMENT APPLYING TO ALL TECH SOLUTIONS				
1. Is the Pandemic Tech Solution centralized or decentralized?				
2. What is the level of internal support, including financial, for the Pandemic Tech Solution?				
3. Who will be accountable within the Project Owner with regards to the Pandemic Tech Solution? Is there a central coordinating body? Who will be accountable within the Project Owner upon failure of the Pandemic Tech Solution, or upon production of adverse outcomes for its users?				
4. What are the roles played by the Project Owner within the Pandemic Tech Solution pipeline (end-user, developer, data provider, etc.)?				
5. Is there an independent commissioner committed to the review and control of such Pandemic Tech Solutions? (e.g. governmental agency, designated official)				
6. Will the staff be trained to use the Pandemic Tech Solution? Are the relevant personnel and/or departments fully aware of their roles and responsibilities? This inquiry should account for different types of staff and the different layers of personnel involved in the design of the Pandemic Tech Solution (e.g., management / oversight in addition to programming levels).				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
7. How will the internal use of the Pandemic Tech Solution by the Project Owner affect the roles and tasks of employees?				
8. What elements of the training and development "supply chain" have been outsourced? If handed off to a third party, are their services subject to the same levels of quality control as the Project Owner?				
9. To what extent does the Pandemic Tech Solution rely on third party data/systems input? How accountable are those third-party dependencies?				
10. Have external QA/QC control methodologies been observed in the creation of the Pandemic Tech Solution (i.e. ISO 9001)?				
PART II – SPECIFIC ASSESSMENT APPLYING TO AI AND MACHINE-LEARNING BASED SOLUTIONS				
11. If applicable, how will the AI model training and selection process be managed?				
12. If applicable, consider maintenance, monitoring, documentation and review of the AI models that have been deployed.				
13. If applicable, consider the various degrees of human oversight in the decision-making process: a) **Human-in-the-Loop:** This model suggests that human oversight is active and involved, with the human retaining full control and the AI only providing recommendations or input. Decisions cannot be exercised without affirmative actions by the human, such as a human command to proceed with a given decision. (NB: Considering here also the concept of "**Human in the Loophole**" where there is automation bias, anchoring or confirmation bias in respect of the human operative. The human essentially affirming the AI outcome without critically assessing whether it is correct or not). b) **Human-out-of-the-Loop:** This model suggests that there is no human oversight over the execution of decisions. AI has full control without the option of human override. c) **Human-over-the-Loop:** This model allows humans to adjust parameters during the execution of the algorithm.				
14. Does the Pandemic Tech Solution involve development, deployment or use of an AI solution or a combination of the three?				
15. What are the rights and interests at stake when the Pandemic Tech Solution makes an automated decision?				
Principle synthesis • Should notably be considered the governance of the Pandemic Tech Solution and whether it ensures the respect of rights and interests of the users. • Should also be considered the safeguards implemented to ensure independence of the Pandemic Tech Solution.				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
Principle #3: Transparency and Explainability *Project Owners that develop, deploy or use Pandemic Tech Solution systems and any national laws that regulate such use shall ensure that, to the extent reasonable given the circumstances and state of the art of the technology, such use is transparent and that the decision outcomes of the data-driven system are explainable.* Overview of the Principle • The Project Owner should ensure at all times that the Pandemic Tech Solution is transparent, including by means of notifying affected stakeholders of: a) the fact that a Pandemic Tech Solution is being used; b) the intended purposes of the Pandemic Tech Solution; and c) the identity of an individual who can respond to questions regarding the Pandemic Tech Solution. Transparency can be reinforced through the concepts of explainability, repeatability and traceability. • The intensity of the transparency and explainability obligations will depend on a variety of factors, including the nature of the data involved, the result of the decision and its consequences for the affected individual. Project Owners that develop Pandemic Tech Solution should ensure that the system architecture, algorithmic logic, data sets, testing methods, and all related development and operational policies and procedures serve to embed transparency and explainability by design.				
PART I – GENERAL ASSESSMENT APPLYING TO ALL TECH SOLUTIONS				
1. Are clear and readable Terms of Use provided to users of the Pandemic Tech Solution?				
2. Do the Terms of Use include data sharing mechanisms? Are there any inconsistencies between what is stated in the Terms of Use and the identified functioning of the Pandemic Tech Solution?				
3. Is a Privacy Policy available?				
4. Does the Project Owner provide information on the scale of adoption? Is there such information available outside of the Project Owner?				
5. Is the Project Owner transparent about the outcomes of the Pandemic Tech Solution? (e.g. false positive or false negative rates of a contact-tracing app...)				
6. Does the Project Owner know what data is used in the Pandemic Tech Solution and how that data is used to arrive at a decision? Would the Project Owner be able to explain the Pandemic Tech Solution to the public?				
7. Does the original data include proprietary information?				
8. Does the original data include anonymised or synthetic data? Would the Pandemic Tech Solution outcome be more accurate/beneficial/less risk of bias if it had included personal information?				
9. Does the original data include personal information?				
10. Is the Pandemic Tech Solution auditable? Auditability refers to the readiness of a Pandemic Tech Solution to undergo an assessment of its algorithms, data and design processes.				
11. Is the Pandemic Tech Solution robust? Robustness refers to the ability of a computer system to cope with errors during execution and erroneous input, and is assessed by the degree to which a system or component can function correctly in the presence of invalid input or stressful environmental conditions.				
12. Is the Project Owner able or prepared to undertake an assessment of the Pandemic Tech Solution to identify the cause of any discriminatory or adverse outcome produced by the Pandemic Tech Solution?				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
PART II – SPECIFIC ASSESSMENT APPLYING TO AI AND MACHINE-LEARNING BASED SOLUTIONS				
13. What is the general degree of opacity of the Pandemic Tech Solution? (ie to what degree could it be described as a "black box")				
14. What type of AI model was used to create the Pandemic Tech Solution, if any?				
15. Is it possible for a specialist to understand how the Pandemic Tech Solution makes its decisions and how it reached a specific conclusion in a specific case?				
16. Consider designing the Pandemic Tech Solution from the most fundamental level upwards to promote transparency and explainability by design.				
17. What are the risks for the rights and interests of stakeholders of unexplainable AI decisions, if any?				
18. What are the transparency and explainability expectations of the different stakeholders?				
19. What is the degree of sophistication of the persons due to receive the explanation (AI specialist, lay-person, educated lay-person, etc.)?				
20. How useful would be this data for persons outside the Project Owner to understand the AI system and its decisions? Would end-users be incentivised or able to game the Pandemic Tech Solution, if aware of the solution's decision-making process?				
21. Is the Pandemic Tech Solution explainable? The Project Owner should be able to explain to a third party how the Pandemic Tech Solution's algorithms function and/or how the decision making process incorporates model prediction.				
22. Is the Pandemic Tech Solution repeatable? Repeatability refers to the ability to consistently perform an action or make a decision, given the same scenario. The consistency in performance could provide AI users with a certain degree of confidence.				
23. Is the Pandemic Tech Solution reproducible? Reproducibility refers to the ability of an independent verification team to produce the same results using the same AI method based on the documentation made by the Project Owner.				
24. Is the Pandemic Tech Solution traceable? A Pandemic Tech Solution is considered to be traceable if its decision-making processes are documented in an easily understandable way.				
Principle synthesis · Should notably be assessed the documentation available to users and the degree of clarity of such documentation. · Should notably be highlighted any opacity of whole or part of the Pandemic Tech Solution. · Should also be summarized the choices made by Project Owner regarding datasets used for the Pandemic Tech Solution.				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
Principle #4: Fairness and Non-Discrimination *Project Owners that develop, deploy or use Pandemic Tech Solution and any national laws or internationally recognized standards that regulate such use shall ensure the non-discrimination of data-driven outcomes, and shall promote appropriate and effective measures to safeguard fairness in use.* Overview of the Principle • The use of the Pandemic Tech Solution should be non-discriminatory in terms of accessibility. The Pandemic Tech Solution should be accessible also to people with disabilities (such as, for instance, limited visual capacity). • Decisions based on the Pandemic Tech Solution should be fair and non-discriminatory, judged against the same standards as decision-making processes conducted entirely by humans. AI development should be designed to prioritize fairness. • This would involve addressing algorithms and data bias from an early stage with a view to ensuring fairness and non-discrimination.				
PART I – GENERAL ASSESSMENT APPLYING TO ALL TECH SOLUTIONS				
1. Is the data high quality data? The following factors should be assessed: – the accuracy of the dataset, in terms of how well the values in the dataset match the true characteristics of the entities described by the dataset; – the completeness of the dataset, both in terms of attributes and items; – the veracity of the dataset, which refers to how credible the data is, including whether the data originated from a reliable source; – how recently the dataset was compiled or updated; – the relevance of the dataset and the context for data collection, as it may affect the interpretation of and reliance on the data for the intended purpose; – the integrity of the dataset that has been joined from multiple datasets, which refers to how well extraction and transformation have been performed; – the usability of the dataset, including how well the dataset is structured in a machine-understandable form; – the usability of any personal information contained within the data sets, including with regards to obtaining any requisite consents; and – human interventions, e.g. if any human has filtered, applied labels, or edited the data.				
2. Consider minimizing inherent bias: – Selection Bias: This bias occurs when the data used to produce the Pandemic Tech Solution are not fully representative of the actual data or environment that the Pandemic Tech Solution may receive or function in. Common examples of selection bias in datasets are omission bias and stereotype bias. – Measurement Bias: This bias occurs when the data collection device causes the data to be systematically skewed in a particular direction. – The following factors should be assessed: • the frequency with which the dataset is reviewed and updated; • the diversity of the dataset, and the variety of sources from which the data has been collected (i.e., numeric, text, audio, visual, transactional etc.); and • the usability of different datasets, including how those datasets have been matched and cleaned so that relational datasets can be correlated and linked.				
3. Is the Pandemic Tech Solution making automated decisions affecting the rights and interests of individuals or businesses – Should notably be considered whether the Pandemic Tech Solution may have consequence for the user to suffer differential treatment which would otherwise be prohibited under any applicable law.				
4. Is the use of the Pandemic Tech Solution voluntary, incentive or compulsory?				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
5. Is there rigorous testing of the Pandemic Tech Solution, both before use and periodically afterwards, to ensure that there is no disparate impact on a protected class of individuals?				
6. May the Pandemic Tech Solution exclude some categories of people from using it? – Have design features contemplated needs of the elderly (for example, ease of use)? – Have design features contemplated the needs of people with disabilities: See: World Wide Web Consortium's Web Accessibility Initiative				
7. Does the Project Owner have in place a system to respond to and resolve situations in which the Pandemic Solution produces discriminatory or unfair outcomes? – This should encompass the Project Owners' capacity to assess and identify biased datasets, potential relief measures provided to end-users and any scope to re-design the Pandemic Tech Solution.				
PART II – SPECIFIC ASSESSMENT APPLYING TO AI AND MACHINE-LEARNING BASED SOLUTIONS				
8. What methodologies have been applied and used in the training of the Pandemic Tech Solution?				
9. Does the Pandemic Tech Solution have a fixed learning phase followed by static use phase or does it continuously improve? If the latter, how are improvements filtered for bias, quality etc.?				
10. What are the risks of bias in 1) the algorithm, 2) the training data, 3) the human developers, 4) end-users?				
11. What are the reputational risks for the Project Owners of the Pandemic Tech Solution making biased automated decisions?				
12. How are "edge cases" managed by the Pandemic Tech Solution?				
13. Is the data used for the training of the Pandemic Tech Solution representative of the population about which the Pandemic Tech Solution will make decisions (data accuracy, data quality and data-completeness)?				
14. Does the Project Owner have an established and robust selection process in relation to the datasets training the Pandemic Tech Solution? For example, are there minimum requirements as to the diversity and quality of the datasets used?				
15. Does the Pandemic Tech Solution use different datasets for training, testing and validation? Weighting Bias: This bias occurs when the data used by the AI Solution are attributed differing weights in producing the relevant outcome. The datasets might be afforded greater or lesser value, which might be arbitrarily or inaccurately awarded.				

Principle synthesis

- Summarize inherent biases of the Pandemic Tech Solution, if any.
- Should notably be assessed any identified discrimination or potential restriction of use for certain categories of persons.
- Should notably be addressed the risk of having derivative misusage of the Pandemic Tech Solution.

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
Principle #5: Safety and Reliability *Project Owners that develop, deploy or use Pandemic Tech Solution and any national laws that regulate such use shall adopt design regimes and standards ensuring high safety and reliability of data-driven systems on one hand while limiting the exposure of developers and deployers on the other hand.* Overview of the Principle The Project Owner should test the Pandemic Tech Solution thoroughly to ensure that it reliably adheres, in operation, to the underpinning ethical and moral principles and has been trained with data which are curated and are as 'error-free' as practicable, given the circumstances.				
PART I – GENERAL ASSESSMENT APPLYING TO ALL TECH SOLUTIONS				
1. In case the Project Owner does not hold international recognized information security certifications (such as ISO/IEC 27001), what is the current level of the security measures adopted? It should notably be assessed the following measures: security incident detection, response and management, business continuity plans, change management policies.				
2. What is the Project Owner's history of data breaches and incidents? How has the Project Owner responded to data breaches and incidents in the past?				
3. What are the cybersecurity risks and vulnerabilities of the Pandemic Tech Solution? Who is at risk of harm? What preventative measures are in place?				
4. Regarding people accessing the data, is confidentiality ensured?				
5. What are possibilities for subversion of intended use? (i.e. where the technology is capable of "dual use")				
6. What are the safety and reliability expectations of the clients and what are their level of sophistication?[1]				
7. What information relating to secure software development and implementation of encryption measures at rest and in transit are provided?				
8. What are the availability and effectiveness of redress mechanisms?				
PART II – SPECIFIC ASSESSMENT APPLYING TO AI AND MACHINE-LEARNING BASED SOLUTIONS				
9. What are the risks of a technical failure of the Pandemic Tech Solution? What are the risks of inaccurate results, polluted datasets, and misuse?[2]				
Principle synthesis • Should notably be summarized and assessed all the technical and organizational measures taken to ensure the safety of the Pandemic Tech Solution.				

[1] Supra note 11.
[2] Supra note 5.

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
Principle #6: Open Data, Fair Competition and Intellectual Property *Project Owners that develop, deploy or use data-driven systems and any national laws that regulate such use shall promote open source and decentralized frameworks. Project Owners that develop, deploy or use Pandemic Tech Solution should take necessary steps to protect the rights in the resulting works through appropriate and directed application of existing intellectual property rights laws.* **Overview of the Principle** • The Project Owner should assess how its Pandemic Tech Solution and its outputs can be used in other pandemic situation or by other Project Owner. • Project Owners must be allowed to protect rights in Pandemic Tech Solution. However, care needs to be taken not to take steps which will amount to overprotection, as this could prove detrimental to the ultimate goal of IP protection.				
1. Is the Pandemic Tech Solution open-source?				
2. Are some use restrictions made clearly public? (e.g. for open-source solutions)				
3. Does the Pandemic Tech Solution offer portability easily?				
4. What is the scope of interoperability with tech solutions offered by other providers?				
5. When developing "heat maps" or related projects, are data sharing is based on anonymized data?				
6. Is the data generated by the Pandemic Tech Solution reusable for other public interest (data for good) projects?				
7. What are the ownership or intellectual property rights attaching to the Pandemic Tech Solution?				
8. Are there any compulsory licensing or patent rights issues relating to the Pandemic Tech Solution?				
9. Have the intellectual property rights attaching to the Pandemic Tech Solution been made publicly available (i.e., turning the underlying code into an open source program)?				
10. Alternatively, are there any obligations or expectations around the provision of the underlying code or software to the public or government entities? If so, will there be any measures regarding adequate remuneration for Project Owners that make such contributions?				
Principle synthesis • Summarize the rights and restrictions attached to the use of the Pandemic Tech Solution.				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
Principle #7: Privacy *Project Owners that develop, deploy or use Pandemic Tech Solution and any national laws that regulate such use shall endeavour to ensure that data-driven systems are compliant with privacy norms and regulations, taking into account the unique characteristics of data-driven systems, and the evolution of standards on privacy.* Overview of the Principle The Project Owner should consider implementing operational safeguards to protect privacy such as privacy by design principles that are specifically tailored to the specific features of deployed the Pandemic Tech Solution.				
1. Are the principles of necessity, proportionality and data minimization fully integrated?				
2. What privacy by design measures have been implemented?				
3. Are personal data that are being collected by the Pandemic Tech Solution used for any secondary purposes during or after the pandemic? Are secondary use of data compatible with initial purposes, if any?				
4. How are transfers of data of the Pandemic Tech Solution outside of the EU/national/regional frontier organized?				
5. What is the Project Owner's lawful basis for processing personal information? What measures does the Project Owner take to ensure compliance?				
6. Who were the data subjects? What type of information was collected about them? What is the scope of the consents obtained?				
7. Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws?				
8. What is the nature of the Project Owner's relationship with the data subjects? How much control will they have? Would they expect you to use their data in this way?				
9. Is sensitive data collected? If so, are there higher standards being adopted for protection of this kind of data?				
10. How was the data used by the Pandemic Tech Solution collected and stored? Was the data transferred by third parties or will the data be transferred to third parties? – Consider whether preprocessing activity has been done on the data before the analysis and whether it would have affected the accuracy and appropriateness of individuals				
11. Are there viable alternatives to the use of personal information? (e.g. anonymization or synthetic data If so, what mechanisms/ techniques are implemented to prevent from re-identification?				
12. Consider if the data is provided by the individual (originated in direct action taken by the individual) and whether: – The data is initiated (the product of individuals taking an action that begins a relationship) – The data is transactional (created when the individual is involved in a transaction) – The data is posted (created when individuals proactively express themselves)				

[3] Ibid.

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
13. Consider if the data is observed (created as the result of individuals being observed and recorded), whether: – The data is engaged (instances in which individuals are aware of observation at some point in time) – The data is not anticipated (instances in which individuals are aware there are sensors but have little awareness that sensors are creating data pertaining to the individuals) – The data is passive (instances in which it is very difficult for the individuals to be aware they are being observed and data pertaining to observation of them is being created)				
14. Consider if the data is derived (created in a mechanical fashion from other data and becomes a new data element related to the individual), whether: – The data is computational (creation of a new data element through an arithmetic process executed on existing numeric elements) – The data is notational (creation of a new data element by classifying individuals as being part of a group based on common attributes shown by members of the group)				
15. Consider if the data is inferred (product of a probability-based analytic process), whether: – The data is statistical (the product of characterization based on a statistical process) – The data is advanced analytical (the product of an advanced analytical process)[3]				
16. Beyond the data subjects' privacy, may the privacy of an identified group be at risk?				
17. Are there procedures for reviewing data retention and performing destruction of data used by the Pandemic Tech Solution? Are there oversight mechanisms in place?				
18. Does the Pandemic Tech Solution provide a functionality allowing the user to "turn-off" the app for a limited time?				

Principle synthesis
• Summarize how personal data protection and privacy principles are addressed by Project Owner:
– Data subjects;
– Categories of data;
– Rights and exercise;
– Potential conflict with Group Privacy.				

4. RISK ASSESSMENT SUMMARY

This section describes the risks you've identified through the PIA process and how you propose to mitigate and manage those risks. It can be useful to link this back to the principles to show why these risks and the proposed actions are relevant. Document the risks in line with any existing risk management processes the Project Owner has – it will be more efficient than trying to run a separate process.

5. RISK MITIGATION ACTION PLAN

This section describes how you propose to mitigate and manage the risks previously described. In some cases, it may be helpful to categorize these actions into areas such as: **Governance / People / Process / Technology**.

Please provide details of all such strategies. Also, please identify the likelihood (low, medium, or high) of this risk happening and the degree of impact it would have on individuals if it occurred. You can use the form of table below.

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.				
2.				
3.				
4.				
5.				