Vodafone Group Response: Consultation on the White Paper on Artificial Intelligence - A European Approach

Executive Summary

Vodafone's response to the AI white paper consultation sits within the wider plan we have established for supporting Europe through the Coronavirus crisis. In addition to our five point plan to respond to the immediate health crisis, Vodafone has developed a long term package of measures to assist with the recovery from the protracted economic crisis we are entering into.

Adoption of AI and data driven tools is a vital part of this strategy and Vodafone wholeheartedly supports the objective of the European Commission to encourage the development of an ecosystem of excellence and an ecosystem of trust for AI development and adoption in Europe. We consider that increased use of AI and data driven technology is a necessary precondition for establishing a resilient European digital society.

Vodafone's objectives for creating a resilient European digital society prioritise a number of key areas:

- Expand and future-proof our network infrastructure through 5G deployment and next-generation fixed line technologies.
- Further support Governments, as they seek to integrate eHealth and eEducation solutions, into their "new normal" public service frameworks.
- Ensure those most vulnerable get the digital access they need and support in digital literacy.
- Promote the widespread adoption of digital technologies for all businesses, with a particular emphasis on SMEs.
- Support Government exit strategies through targeted deployment of digital technology.

These would be transformational steps with long-lasting positive effects for societies. This agenda complements our continued delivery on Vodafone's purpose targets, including halving our carbon emissions and sourcing 100% renewable electricity by 2025, as well as helping our customers to reduce their environmental impact through our products and services (not least IoT, such smart logistics and fleet management, and smart metering). For example, last year in Europe, we helped our customers save five times the emissions generated from our own operations.

As a result, we believe these actions align fully with the Commission President's vision of building a resilient, green and digital Europe. However, we will not be able to do this alone. In order to achieve our objectives and the actions set out above, Governments will need to make a step change in their support for the vulnerable and small businesses including in terms of digitisation.

Throughout the first phase of our response AI and data driven modelling have been used to assist governments in mapping the spread of the Coronavirus under different conditions, informing policy decisions to bring the spread of the virus under control. As we look towards exiting the lockdown and restarting economic activity, these insights will be just as crucial in ensuring that governments continue to supress transmission rates and are able to respond and act in real time to changes in the situation.

Epidemiological models benefit from high-quality, real-time data about the number of infected, hospitalized and intensive care individuals. Moreover, human mobility (which can be mapped at an aggregate level through mobile network data) and quarantine information enable the creation of more accurate models and predictions. Having an underlying model enables running it under different scenarios, for example different social concentration, mobility and contact tracing situations, to assess the impact that different interventions might have on the transmission and spread of the infectious disease.

Data and machine learning have been used historically to improve clinical outcomes. In the case of COVID-19, we have witnessed better diagnosis using AI-based diagnostic tools applied on radiological images or better outcome predictions based on the analysis of electronic health records and symptoms. AI is also being applied for improved or quicker diagnosis, to identify drugs to treat Covid symptoms and with the use of robots for delivery of drugs and other resources to hospitals or patients in their homes.

Our response to this consultation underlines the importance of creating an enabling environment for AI applications and services, many of which will be critical to establishing a resilient European digital society. On the key areas of regulation proposed by the Commission, our response can be summarized along the following lines:

- **Regulation of high-risk AI**: We broadly support the approach outlined by the Commission to limit avoid duplication of existing regulatory obligations, and ensure that any new requirements are proportionate and strictly targeted at AI applications that pose a high risk.
- **Voluntary labeling**: We raise particular concerns with the lack of focus given to incentives to develop Trustworthy AI (voluntary labeling, certification, industry codes) and ask for more clarity on how such a labeling scheme would be established and maintained.
- **Product Liability**: we note that the existing EU horizontal and sector-specific legislative framework governing liability has proven to be robust and reliable. Any new requirements should be targeted at providers of high-risk AI applications & must not impose excessive high burdens on industry deploying AI that presents a low risk to EU citizens.
- **Access to data**: we underline the importance of availability of high quality training data for AI, to ensure that European businesses can continue to innovate and succeed in this field, and call for joined up policy making in view of the EU Data Strategy and legislative actions outlined therein.

Ecosystem of excellence

Actions to be undertaken to promote the ecosystem of excellence

We support the actions outlined by the Commission in the White Paper to establish Europe as a frontrunner in AI innovation and development. Working with Member States will be crucial in this regard, to maximise the capacity and investment that exists at a national level, and to share expertise and best practice. In order to compete at the global level, it will also be necessary for European countries to collaborate and pool resources. Above all, the EU should take advantage of its large internal market to ensure that AI products and services (and the companies behind them)

have the opportunity to scale rapidly, and thereby compete with the research and exporting powerhouses elsewhere in the world.

Updating the Coordinate Plan on AI – other actions that should be considered?

The US and China are advancing rapidly in terms of AI innovation and investment. Both benefit from economies of scale stemming from large domestic markets under a unified regulatory framework. To compete on a global scale, the EU must be able to leverage its own resources and those of member states national exchequers to ensure that equivalent capital is invested in indigenous EU AI technology.

EU policy makers should attempt to ensure a harmonized regulatory environment across the EU concerning AI technology to avoid costly fragmentation. The Commission has shown good intent in bringing forward the Coordinated Plan and we urge Member States to follow this approach, coordinating closely in the preparation and implementation of national AI strategies.

Of concern, not all member states have responded to the Coordinated Plan by bringing forward domestic AI strategies/deployment plans, and some of those that have been published are relatively light on detail in terms of concrete measures being taken by the government to boost AI research and innovation and support its adoption. We would like to see the Commission issue a follow up Communication, encouraging those countries who have not brought forward AI strategies to do so expeditiously. It would also be helpful were the Commission to extrapolate key learnings and best practice from members states (what have been the key challenges, where have we seen good success) and to use this to create a set of benchmarks/KPIs for other Member States to target.

Are there any other actions to strengthen the research and innovation community that should be given a priority?

Companies and institutions in Europe from different sectors should be encouraged, supported or incentivised to release or open-source modern and meaningful datasets, which can be used by innovators, researchers and academia to explore advanced AI mechanisms and algorithms in order to tackle new challenges. Without this support in place, any successful release of capital by the EU or individual member states towards development of indigenous EU AI would risk being ineffective.

Are there any other tasks that you consider important for specialised Digital Innovations Hubs?

No Vodafone views

Ecosystem of Trust

Do you have any other concerns about AI that are not mentioned above?

Broadly speaking we agree with the concerns raised by the Commission in relation to AI specific harms. Many of the human rights implications of AI technology are not new, for example, the right to fair treatment access to justice and freedom from discrimination. What is new about AI is the sheer pace and scale of transformation and the fact that decisions and actions which have traditionally only been taken by a human agent will increasingly be supplemented, or at some point in the future entirely replicated by AI systems.

The important thing from a human rights perspective is that where AI systems are deployed to assist in decision making processes, the autonomy, dignity and integrity of human subjects (EU citizens) are respected at all times.

At Vodafone, we are subject to sectoral regulation, horizontal regulatory requirements (such as GDPR) and a host of voluntary and co-regulatory codes of practice. These overlapping measures ensure that everything we do is with respect to fundamental rights.

In addition, we have developed a Vodafone AI Framework, which sets out at a high level how we will deploy AI across our footprint in an ethical manner. The key aspects of this Framework relate to areas where we perceive there to be the greatest risk of harm arising from AI technology:

- transparency & accountability,
- ethics & fairness,
- privacy & security,
- bias & discrimination,
- diversity & inclusivity

Do you think that the concerns expressed above can be addressed by applicable EU legislation? If not, do you think that there should be specific new rules for AI systems?

Vodafone supports the EU ambition to become a global leader in ethical, human-centric AI technology, however we warn against the introduction of prescriptive regulation of all AI, which could hinder some of the innovative AI applications we have developed.

Vodafone supports the conclusions of the AI High Level Expert Group in pursuing a risk-based, innovation first policies, backed up by a strong ethical framework, avoiding the need for heavy-handed regulation. Many uses of AI (such as fault detection in our networks) have no direct impact on individual users and no additional regulation is required. In particular, we would underline the need for a gap analysis against existing laws imposing new transparency/explainability requirements or new liability obligations. For example; data protection requirements already impose obligations to explain how personal data is used, antidiscrimination laws already exist in EU countries explicitly prohibiting direct discrimination against groups based on certain characteristics.

As the Commission has rightly noted, in many cases, the problems presented by AI are not a consequence of a lack of existing legislation, but in consistently upholding and enforcing existing laws when dealing with complex AI systems. For example, it can be difficult to establish accountability and in particular, where decisions may be taken, or assisted by algorithmic decision-making systems. The problems are exacerbated by gaps between national regulatory regimes,

In such circumstances, we agree that certain targeted regulatory requirements could be appropriate for those AI applications that present a high or significant risk to end-users. We elaborate below on the criteria which we believe should be used to determine whether an AI application is deemed to be 'high-risk' and therefore subject to additional regulatory requirements. At a high level, we believe such an assessment should rest on a calculation of the likelihood of

harm occurring, the degree of harm to an individual user and the scale of harm (i.e. number of those who could be affected). In addition, the Commission should also consider a number of other normative requirements for additional obligations to bite, for example the intended purpose of the AI application, the risk level present in a given sector, or the market position of the firm developing the AI application.

If you wish, please indicate the AI application or use that is most concerning ("high-risk") from your perspective:

AI should be considered high risk when it passes a certain threshold, calculated on the basis of; i) potential/likelihood for harm to occur, ii) severity of harm for those affected and iii) number of individuals or legal persons affected by the harm. We also consider that certain sectors may be deemed as high risk when deploying AI and therefore subject to regulation, including healthcare and transport.

Proportionate regulation of AI should be a combination of horizontal and vertical measures – horizontal measures being a requirement to complete a human impact assessment for AI where the application of the AI system presents a high risk to individuals.

In determining the extent to which an AI application constitutes a high risk, we would direct the Commission towards the risk assessment framework contained in the 2019 German Data Ethics Commission report. According to the report: "the level of criticality of an algorithmic system dictates the specific requirements it must meet, in particular with regard to transparency and oversight. System criticality is determined by assessing an algorithmic system's potential for harm, on the basis of a two-pronged investigation into the likelihood that harm will occur and the severity of that harm."

In determining the severity of potential harm caused by an AI application going wrong, a number of underlying considerations are relevant:

- the *significance* of the legally protected rights and interests affected (such as the right to privacy, the fundamental right to life and physical integrity, the prohibition of discrimination)
- the *level* of potential harm suffered by individuals (including non-material harm or loss of utility that are hard to calculate in monetary terms)
- the *number* of individuals affected, the total figure of the harm potentially sustained and the overall harm sustained by society as a whole

In determining the likelihood or probability of harm arising as the result of an AI application malfunctioning or being misused, an additional set of considerations are relevant:

- the *role* of the algorithmic system components in the decision-making process,
- the *complexity* of the decision
- the *effects* of the decision and the reversibility of these effect
- the degree of human oversight of the process in which the AI system makes decisions

The Data Ethics Commission additionally suggests that a number of normative criteria should also be used when determining the level of risk posed by an AI application, for example whether the system is operated by the state (which can give rise to specific concerns around misuse and mission creep) or, if deployed in the private sector, whether the sector of activity in itself presents

a high level of risk (healthcare and transport being two obvious examples where there is a greater risk of material harm). Lastly, we agree with the Data Ethics Commission that additional regulatory requirements for high risk AI could also be appropriate where the provider exhibits systemic or significant market power.

Do you believe that a voluntary labelling system (Section 5.G of the White Paper) would be useful for AI systems that are not considered high-risk in addition to existing legislation?

Voluntary labelling can act as a useful incentive for businesses to adopt best practice, by conferring on them a potential competitive advantage in the marketplace over providers who are not able to meet the thresholds or requirements necessary to obtain such a Trustmark or seal. We think such an approach could have merit in the context of AI, as a means of encouraging best practice for developers of AI which falls below the high risk threshold and is therefore not subject to mandatory (ex-ante) legal requirements outlined in the white paper.

However, we are disappointed that more attention has not been given to this strategy in the white paper, where the focus is very strongly on regulation of high risk AI. While there a robust conformity assessment regime is envisaged for developers of AI applications, acting as a disincentive to development of AI that does not have sufficient safeguards built in, not enough attention has been given to potential *incentives* for AI developers.

For example, the Commission could borrow from the detailed guidance developed by the High Level Expert Group for Trustworthy AI, and look to offer a formal certification or approval processes for companies who want to undertake the voluntary assessment list contained in those guidelines. Any such process should be straightforward, easy to comprehend and result in a labelling system that confers genuine benefits on diligent operators.

What is the best way to ensure that AI is trustworthy, secure, in respect of European values, and rules?

Vodafone is supportive of the development of ethics guidelines for trustworthy AI and has participated in the pilot process of the AI HLEG Ethics Guidelines for Trustworthy AI, recently offering our detailed feedback on the assessment list contained in section three of those guidelines. In our view the ethics guidelines are a good starting point in terms of creating a consensus around the development of AI that is trustworthy by design, and there is a good degree of alignment with the Vodafone AI Framework.

Our response to the HLEG focused on ensuring that the assessment list is as concise and understandable as possible for people working in product development and technical roles and does not unnecessarily duplicate existing functions and processes. We look forward to reviewing the final draft of the HLEG ethics Guidelines on Trustworthy AI, included updated assessment list to check if our comments have been reflected. If so, we are confident that this document can be a useful tool for businesses looking to embed ethics by design and Trustworthiness into their AI product development cycles.

Beyond this, in creating an Ecosystem of Trust, we would direct the Commission towards a number of overarching principles:

- Only adopt new regulation where clear gaps in relation to the existing legal framework at both the EU and national level have been identified.

- Adopt a principles-based and outcome-based regulatory approach.
- Consider all GDPR provisions that already regulate AI, including obligations of fair processing, transparency, accountability, regulatory oversight, right to redress of individuals and liability.
- Enable organisations to develop their own tools or leverage their existing tools to assess the impact of AI holistically, including individual and societal risks, benefits and risk profile.
- Acknowledge that by providing for general obligations of fair processing, transparency and accountability, GDPR provides a robust framework on transparency in the AI context. Leverage existing GDPR rules and tools to foster accountable data sharing.
- Promote creative, forward-thinking and progressive interpretation of current GDPR requirements by regulators.
- Acknowledge organisations' emerging accountable AI best practices in the EU to address the risks and benefits of AI.
- Embed "organisational accountability" as the key element of the EU approach to AI to foster trust and sustainable AI practices[1]
- Provide incentives for organisations, in both the public and private sector in the EU, to develop accountable frameworks for AI.
- Provide solutions to address conflicts of laws and enable regulators to collaborate through regulatory hubs to ensure that AI benefits from a clear and consistent legal framework, for example looking at the way in which data protection regulators are able to collaborate and share best practice via the European Data Protection Board.

Safety and liability implications of AI, IoT and robotics

The current product safety legislation already supports an extended concept of safety protecting against all kind of risks arising from the product according to its use. However, which particular risks stemming from the use of artificial intelligence do you think should be further spelled out to provide more legal certainty?

As AI grows in usage and impact across geographies and industries, Vodafone has a responsibility to consider how our use of this technology affects our customers, our employees, and wider society. Vodafone supports the EU ambition to become a global leader in ethical, human-centric AI technology. We support the Commission in conducting a thorough assessment of the application of existing EU liability rules to determine if they remain fit for purpose in the context of AI decision making.

In your opinion, are there any further risks to be expanded on to provide more legal certainty?

We strongly support the Commission appointed Expert Group on Liability for AI and other emerging technologies in their rejection of the European Parliament resolution calling for AI systems to be granted legal personhood. Such a move would not be productive in helping to apportion liability for harm caused by AI, and would could create significant confusion and uncertainty about the respective roles of those developing and operating AI technology.

We note that existing EU horizontal and sector-specific legislative framework governing liability is robust and reliable, since the current definition of product safety already includes an extended

[1] CIPL White Paper - What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework
May 27, 2020

concept of safety, and that liability issues are generally covered by the liability concept already in place. Any additional requirements should only apply to high risk applications, and should aim at providing confidence and certainty for those operating AI technology, but also for businesses such as ours who are increasingly utilising AI in their daily operations and customer services.

Do you think that the safety legislative framework should consider new risk assessment procedures for products subject to important changes during their lifetime?

Vodafone supports the introduction of new risk assessments procedures for products that are subject to important changes during their lifetime to ensure, for example, that relevant security updates and software patches have been applied. A focus on procedural risk assessment will help to distribute responsibility for an AI product or system across the whole value chain, and introduce necessary transparency to ensure that additional obligations are appropriately targeted at those best placed to act.

In addition, we believe that such an approach should take into account the risk levels involved. For example connected or autonomous vehicles, whose operation poses a significant risk of harm to individuals should be subject to more frequent and more detailed risk assessment procedures than operators of an AI system deployed within a customer care channel, where the associated risk level is much lower.

Do you think that the current EU legislative framework for liability (Product Liability Directive) should be amended to better cover the risks engendered by certain AI applications?

We underline the fact that a functioning liability system for AI needs to strike a careful balance between on the one hand providing assurances for users of AI, while avoiding introducing a level of liability for the producers and developers of AI technology that is prohibitive or discourages innovation in this area. Europe will certainly not be able to keep pace with the levels of AI innovation in the US and China if all developers are saddled with strict liability for harm occurring only tangentially as a result of AI technology they deploy. We outline a number of key considerations for the Commission in bringing forward any changes to the current product liability framework.

- Any new requirements should be targeted at **providers of high-risk AI applications** & must **not impose excessive** high burdens on industry deploying AI that presents a low risk to EU citizens.
- It should be considered that liability in B2C relations that goes beyond contractually agreed terms is **also ensured by other consumer law** such as the Sales of Goods Directive (goods: security updates, and software essential for functioning of goods) and the Digital Content Directive (applicable to content/ services: software and security updates) and national civil/commercial law, where applicable
- **The Commission should strive towards better distribution of liability along the value chain** through stronger focus on producers, to better reflect principle of responsibility and to enable traders fulfilling contractual obligations
- **Gaps for responsibility** along the value chain remain e.g. **Cybersecurity:** Limiting liability to the traders in case of B2C issues not only impose unfair burdens on traders but also hampers the provision of security safeguards to consumers
- Any new laws should take into account **failure of the injured party** to download updates e.g. security updates.

Do you think that the current national liability rules should be adapted for the operation of AI to better ensure proper compensation for damage and a fair allocation of liability?

The Product Liability Directive has proved a durable and adaptable instrument. In general, Vodafone would support greater harmonisation of liability regimes across the single market, to reduce the costs of fragmentation for businesses and ensure a universal level of protection for consumers. As such, it would be appropriate for the Commission to conduct a thorough revision of national liability regimes in light of the challenges posed by AI raised above and to propose potential modifications to update and harmonise these rules, in view of technological developments.

IoT

Liability (along with security) are cross border issues; a harmonised approach to product liability is key in order to avoid stifling innovation by creating an uncertain, inefficient and/or unworkable regulatory context. Vodafone has put forward a detailed description of policy measures necessary to unleash IoT innovation in Europe in the white paper a New IoT Regulatory Framework for Europe.[2] Here we describe how to address potential issues around liability: "participants in the IoT value chain should ensure contractual arrangements between them are clear in relation to which party is responsible in the event that an IoT-enabled product causes damage".

Key to this vision is increased transparency in relation to liability – this can address the concerns without imposing disproportionate liability requirements. This ensures consumer trust and engagement that are essential. As such IoT liability rules should ensure that consumers are clearly informed on who is responsible for the development and operations of different aspects of an IoT solution, including hardware, software and connectivity and who they should contact in the event of harm.

In IoT complex use cases (e.g. Smart Home) there is role to be played by the development of globally aligned safety standards. Furthermore we believe that issues within B2B relations can be satisfactorily and appropriately addressed through, commercial contractual arrangements (i.e. the approach that industry is currently taking when pairing up IoT products and services); therefore, B2B should not be in the scope of discussions.

[2] https://www.vodafone.com/content/dam/vodcom/files/public-policy/iot-whitepaper/IoT_whitepaper_.pdf