Versatile artificial intelligence investigative technologies for revealing online cross-border financing activities of terrorism

D1.3 Anti-FinTer Ethical Requirements and Code of Conduct

WP number and title	WP1 – Project Management
Deliverable number	D1.3
Version Number	1.0
Document Reference	Anti-FinTer Ethical Requirements and Code of Conduct
Lead Beneficiary	ULIM
Deliverable type	Report
Planned deliverable date	2022-03-31
Date of Issue	2022-03-31
Dissemination level	PU
Authors	Dr Martin Cunneen
Contributor(s)	
Keywords	Data Governance, Data Ethics and Research Ethics

This project has received funding from the European Union's ISFP-2020-AG-TERFIN program under the Grant Agreement No. 101036262

Consortium Partners

The Anti-FinTer Consortium consists of the following partners:

Participant No	Participant organisation name	Short Name	Country
1	AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH	AIT	Austria
2	IDRYMA TECHNOLOGIAS KAI EREVNAS	FORTH	Greece
3	FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUALY COMUNICACIONES VICOMTECH	VICOM	Spain
4	IANUS CONSULTING LTD	IANUS	Cyprus
5	CFLW CYBER STRATEGIES BV	CFLW	Netherlands
6	UNIVERSITY OF LIMERICK	ULIM	Ireland
7	FINANSINIU NUSIKALTIMU TYRIMO TARNYBA PRIE VIDAUS REIKALU MINISTERIJOS	FCIS	Lithuania
8	AGENCIA ESTATAL DE ADMINISTRACION TRIBUTARIA	AEAT	Spain
9	Ministério da Justiça	MJPJ	Portugal
10	GLAVNA DIREKTSIA BORBA SORGANIZIRANATA PRESTUPNOST	GDCOC	Bulgaria

Document History

Version	Date	Status	Author(s), Reviewer	Description
V0.1	2022-03-18	Draft	Martin Cunneen (ULIM)	Initial Draft
V0.2	2022-03-23	Reviewed	Mark van Staalduinen (CFLW)	Reviewed version
V0.3	2022-03-25	Reviewed	Martin Cunneen (ULIM)	Upated based on review commnets
V0.9	2022-03-29	Released	Martin Cunneen (ULIM)	Final version
V1.0	2022-03-31	Final	Ross King (AIT)	Submitted version

Definitions, Acronyms and Abbreviations

Acronyms/ Abbreviations	Description
DeFi	**Decentralised Finance**
LEA	**Law Enforcement Agency**
AFT	**Anti-FinTer**
PET	**Privacy-Enhancing Technologies**
RRI	**Responsible Research and Innovation**
GDPR	**General Data Protection Regulation**

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Purpose of the Document (Introduction)

Following the 2008 financial crash, the first cryptocurrency, Bitcoin, was proposed as an alternative financial instrument [1]. Subsequently, cryptocurrencies have become a shadow global financial system now offering Decentralised Finance (DeFi) as the latest phase of the unregulated market, adopting practices previously only available in the highly regulated world of financial institutions and global finance. Hence, cryptocurrencies have become a resource for carrying out financial transactions that are often not within the surface systems of financial institutions. Accordingly, this hidden and quasi anonymisation has proven lucrative to criminals and terrorists to transfer funds and purchase goods away from the scope of Law Enforcement Agencies (LEAs).

Anti-FinTer (AFT) aims to build upon previous research to provide innovative solutions and strategies encapsulated in tools that are built upon combining proven solutions relating to cryptocurrency analytics supplemented with graphsense data capture and the general processing of public data.[1] The project will provide accessible tools for stakeholders such as LEAs and governmental bodies to monitor and manage risks relating to terrorism and cryptocurrency activities. To achieve reliable and trustworthy tools that produce court-proof actionable insights, AFT must address the catalogue of identifiable and documented risks (see section 2) that undermine the operational use of digital forensics and crypto forensic tools. In particular, technical and governance failures could have severe harm on the automated targeting of citizens. Risk relates to this challenging scenario concerning the erosion of protections found in fundamental legal, human rights and civil liberties instruments. Therefore, to support safe and dependable scalable operations, the design and use of AFT tools must be informed by, and adhere to, citizen and human rights charters, legal data governance and ethical governance instruments[2]. Accordingly, successfully responding to the complex data and ethical compliance will ultimately determine the success of AFT tools in design, use and value. Moreover, high profile stakeholders in the EU Law Enforcement and Intelligence ecosystem require AFT to provide robust, dependable, and trustworthy solutions[3].

The use of public and personal data to identify and mitigate socio-economic risks and unlawful activities may seem justifiable, especially when citizens' harm is involved. Such thinking often justifies using public data combined with commercial data analytics strategies to mitigate numerous criminal activities. The use of data analytics, machine learning and AI on publically available data is often packaged as an economical solution to mitigate some criminal activities. However, as Gottschalk identifies, this approach introduces unique risks to LEAs, citizens and broader society[2]. Product design teams need to understand better what they cannot safely do with data analytics (Research Ethics and Integrity), what they are not allowed to do (Data

[1] There are concerns regarding the lack of a clear definiton and statement in legal instruments reating to the meaning of 'public data'. Gottschalk (2020) makes this an explicit component of his critical analysis given that regulatory instruments remain unclear regarding "Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives".

[2] At a foundational level EU research and especially EU funded research must be informed by and adhere to article 19 Regulation(EU) n. 1291/2013 (Horizon 2020): "all the research and innovation activities carried under Horizon 2020 shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols. Particular attention shall be paid to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection."

[3] These include the European Anti-Cybercrime Technology Development Association (EACTDA), a non-profit organization whose goal is the development of technological solutions for European LEAs and Forensic Laboratories to use them in their fight against crime. Moreover, tools will be operationalised and may be made more available through international organizations such as Europol, CEPOL, FRONTEX and the United Nations.

Compliance) and what they ought not to do (Data Ethics). These three questions need embedding into developmental phases of data analytics solutions that concern citizen data and especially scraped public domain data relating to citizens. This relates to what Rios and Lopez describe as a natural conflict between digital forensics practices, the more recent subdomains of surface web and crypto forensics, with privacy and privacy rights[3]. Moreover, as Simon Hale-Ross asserts, the difficulties align with a challenge between collective security and privacy. Hence, the challenges and difficulties are commonly acknowledged, and some have taken progressive actions to support data forensics and crypto forensics strategies by addressing them with informed strategies[4, 5]. Accordingly, D1.3 also follows this innovation pathway to support the development of informed solutions by assessing and strategically mitigating the risks.

Robust data compliance is dependent upon several variables relating to data capture, categorisation, processing, analytics and network forensics [6] to achieve trustworthy outputs (actionable insights) [7]. As experts in data forensics, law enforcement and crypto forensics point out, there is a need for robust and informed data governance, compliance, and ethical assessment to support research and project integrity [6-8]. Moreover, a robust compliance regime coupled with a strong respect for privacy and privacy guarantees [3] is necessary to achieve nominal technological functionality and design proficiency. Accordingly, for crypto forensics-based methodology and technology-based solutions to offer stakeholders such as LEAs intelligence and risk mitigation benefits, the intelligence must achieve a data and ethics compliance rigour that can stand up in a court of law by providing court-proof evidence [9]. This could mean that clear and concise legal and ethical compliance evidence is an essential requirement. Prosecutors require clear and informed operational compliance in both the design and use of data forensics tools in order to achieve the necessary robustness thresholds for quality, veracity-enabling, trustworthy, actionable intelligence. D1.3 aims to transform the data risk aspects of crypto forensics from a multitude of complex risk challenges into a manageable risk environment. Accordingly, ULIM uses D1.3 to provide the foundation of a strategic risk management regime to capture, counter and mitigate compliance and ethical risks and provide continued support to stakeholders to sustain the risk management strategies. The data risk management regime is built upon a foundation of data provenance[4] that is operationalised across two community contexts that promote data-responsible professionals. Therefore, the first community represents (1) the design and development community and (2) the deployment, operations and end-user communities. Furthermore, to support activities to promote a more robust and sustainable data provenance culture, D1.3 utilises (a) EU research ethics, (b) Data Governance, Data ethics and privacy-enhancing tools (including the use of a digital evidence management framework (DEMF[8]) and (c) a context code of conduct for the use of AFT tools.

1.2 Structure of the Document

The document is built on four sections. Each section provides a pillar to the overall output of the best practices methodology informed by research ethics, data governance and data ethics. The pillars act as supports to enable more informed decision-making along the innovation pipeline of AFT from development to deployment phases.

The document consists of the following four sections:

Section one
Contextualises the challenge (risk and ethical) space of AFT tool development (as a complex, multilayered data risk context for innovations in crypto forensics) and the required effective and compliant use of the tools by stakeholders.

Section two

[4] Data Provenance is the historical record of the data, its orgins and changes. It is sometimes constructed as a ledger recording the changes to data as it is processed.

Appeals to and adapts the EU charter on research ethics as a primary support to inform and guide AFT research activities and decisions.

Section three
Assesses data governance and ethics to develop a strategic approach to utilising optimal privacy-enhancing technologies (PET) to strategically address the requirements and compliance opportunities relating to core data governance mechanisms and instruments.

Section four
Sets out the foundation to develop and operationalise a code of conduct for the use of AFT tools

The four sections collectively provide a positive response in capturing the complex risk environment of crypto forensics innovation for LEAs and use this analysis to formulate a strategic risk management regime informed by data governance and ethics. Moreover, the regime focuses on practical solutions to support context-specific risk mitigation and continued sustainable and adaptable risk mitigation.

1.3 Scope and Intended Audience

For the first half of the project, D1.3 is primarily inward-facing in its goal to provide consortium members with guidance on research practices, ethics, and data compliance guidelines.

In a secondary context, in the latter half, it is outward facing by designing and operationalising an informed and context-specific code of conduct for the use of the AFT tools and methods by third-party stakeholders and users.

1) Research Ethics, Compliance and Best Practices (Project Participants)
    a) Research Ethics and EU Research Code of Conduct
    b) Data Compliance Assessment
    c) Data Management Plan (DMP)

2) Proposed Solutions (Tools and services) Ethical Assessment and Operational Guidelines (First Line Practitioners)
    a) Ethical analysis of proposed solutions, tools and services
    b) Hard and soft data governance instruments are processed to support analysis and guidelines
    i) General Data Protection Regulation
    ii) Data Governance Act
    iii) Digital Services Act
    iv) Digital Markets Act
    v) Data Act
    c) Citizen and human rights inform the analysis and guidelines
    i) The European Charter of Fundamental Rights
    ii) The European Convention on Human Rights

3) AFT Tools and Services Code of Conduct (Developers and End Users)
    a) The code of conduct will be informed through enagement with the project community. A risk and anticiaptory governance context of analysis will inform the final iteration of the code.

2 Assessing the Risk and Ethical Space of Crypto Forensics Innovation

There are strategically important resources of research available from academia and especially from previous EU projects in digital forensics, crypto forensics, deep web monitoring, surface web analytics, and innovative strategies that create new data and analytics responses. Four previous EU-funded projects provide a great deal of informative guidance regarding the risk and ethical space of crypto foresenics as strategies to support LEAs in their activities to identify and mitigate the risks relating to criminal and terrorist use of cryptocurrencies[5].

Several other research projects in this domain (Titanium, Asgard, Trust and Starlight) highlight both opportunities and questions that remain to be answered regarding the effectiveness of crypto forensics for LEAs, given the significant challenges and risks the strategy incorporates. Accordingly, a primary challenge is to capture the risk challenges of crypto forensics and to create context-specific and robust risk mitigation strategies. AFT uses D1.3 to address this challenge and provide an informed and robust strategy to mitigate and manage risks to a level that enables cautious use that achieves compliance and ethical use of crypto forensics.

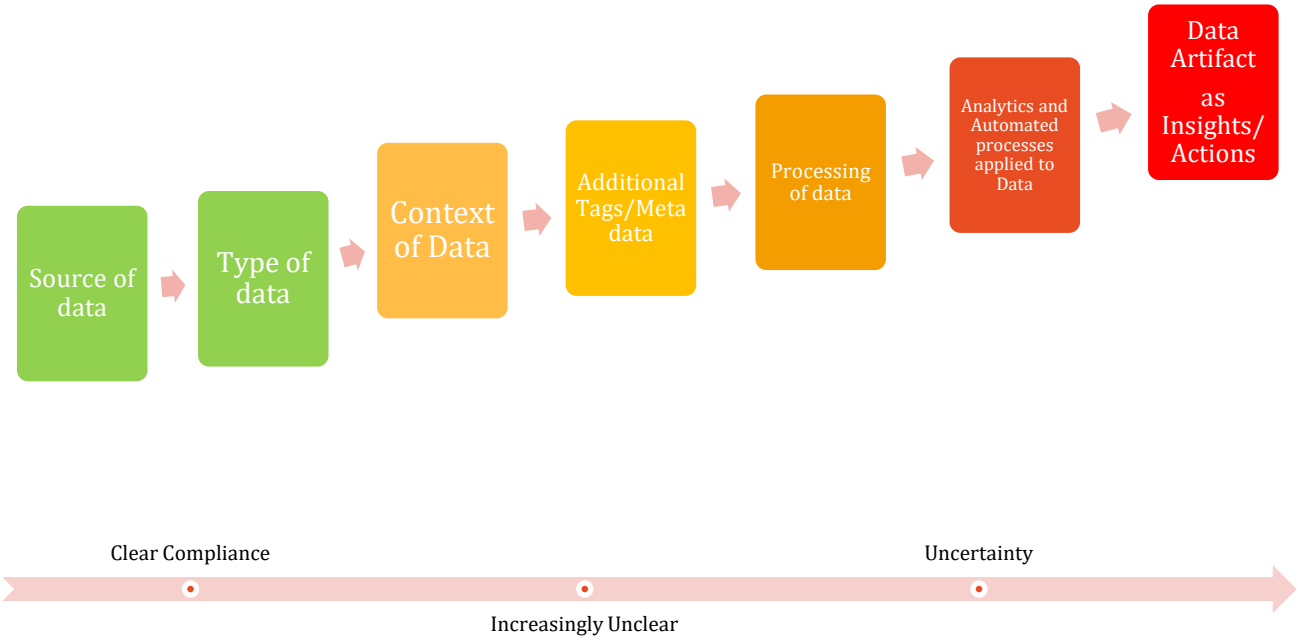

Figure 1: Current crypto forensics approaches to data and ethical compliance

[5] See: Hanrahan, Mark, Jessica Wang, "Number of fatal terrorist attacks in western Europe increasing, data show", Reuters, 12 July 2017. https://www.reuters.com/article/us-europe-attacks/number-of-fatal-terrorist-attacks-in-western-europe-increasing-data-show-idUSKBN19X1QO.

2.1 Cryptoforensic Operational Risk and Risk Mitigation Table

Table 1: Operational Risk and Mitgation Matrix

Risk	Severity	Anti-FinTer Risk Mitigation Response	New Risk Rating
List of risks	Rating	Catalogue of Risk Mitigation Tools	Output
1. Design Risks a) Technical error/faults b) Clustering error risk c) Attribution Tag Risk (Polsemy/Synonymy) d) Unknown unknowns e) Lack of understanding of research ethics f) Lack of understanding of data compliance g) Lack of understanding of data ethics	High	• Transparency and Explainability of Clustering techniques and assessment[6] • Tag data contextual verification before action[7] • Data Auditing through Lineage and Provence techniques provides a more robust and trustworthy data pipeline built on greater authenticity • Research Ethics • Data Governance • Data Compliance • Privacy-Enhancing Tools • Privacy by Design ○ Anonymisation ○ Pseudo Anonymisation ○ Risk Accumulation Thresholds ○ Robust security and access controls • Data/AI Ethics by Design ○ Applied Data/AI Ethics ○ Explainability ○ Transparency ○ Accountability • Technology Assessments • Stakeholder Participation	Caution
2. Operational Risks a) LEAs and stakeholders incorporate tools while unaware of the above risks in 1.	High	• Multi-Stakeholder, LEA and End-user training • Operational and Safety training ○ Data Compliance and Data Ethical training ○ Applied Risk and Ethical training with a focus on operationalising	Caution

[6] See the important analysis on this point in Titanium D3.4 p3: "The reliability of clustering results is of uttermost importance for forensic investigations. Wrong clustering results can lead to missed- or even false convictions. Quantifying the reliability of clustering results is not easy since no ground truth data is available. Furthermore, most clustering heuristics make assumptions about the behavior of participants. Obviously, user behavior can change."

[7] On this point, Titanium D3.4 p3 identifies semantic tagging is highlighted as a constructive response: "As for clustering the reliability of tag data is crucial for investigations. The reliability of tags mainly depends on the origin of the tag as well as its processing history."

b) LEAs fail to have an informed duty of compliance, care and ethics c) End users are not aware of risks presented in 1. d) Operations are carried out in a high-risk environment with stakeholders unaware of the embedded operational risks e) Function creep and mission creep regarding potential misuse of tools f) Ethical risks relate to an ethical burden transferred from lack of ethical design to the end-users and broader society		key ethical principles to inform operational use and decision making • Code of Conduct for End Users	
3. Actionable Risks a) Operations may use data and analytics processes that provide insights/outputs that LEAs trust and take action on innocent people identified as suspects due to technical and data compliance errors. b) Operations may use data and analytics processes that provide insights/outputs that LEAs trust and take actions on but are not compliant with legal frameworks and regulation or ethical ideals such as EU human rights charters. c) Failed processes and prosecutions may lead to significant citizen and social harm in terms of lack of trust and social confidence in LEA using data analytics. d) Citizen welfare, human rights and fundamental privacy rights may be undermined by ill-informed operations that have given rise to real-world actions by LEAs in arresting and attempting prosecutions.	High	The strategies and actions from the above responses (1+2) significantly transform Actionable Risk from high to caution.	Caution

2.2 Data and Ethical Compliance as Risk mitigation strategies to support informed and responsible operations and use of crypto forensics for LEAs

"(LEAs) often put themselves in the hands of external data scientists that lack the necessary knowledge of the legal implications of their approaches in particular when it comes to publicly available data." [2]

As the quotation highlights, research projects have documented in the literature that, sometimes, the designers of such intelligence solutions can lack the necessary understanding of the additional risks and potential harms of their designs and applications [2]. This is most evident in how the use of public data and sensitive citizen data is processed through machine intelligence solutions in the name of innovating law enforcement. It makes sense that law enforcement can access data-centred innovations and solutions promising risk mitigation benefits. That said, the use of data analytics solutions by LEAs does come with some costs, risks and challenges. The most apparent cost and related ethical tension concern the use of public funds to purchase private data analytics products and services for surveillance of EU citizens. Moreover, there are a wide array of related risks ranging from infringement of human rights, privacy erosion, and failed data regulation compliance to prosecution cases failing due to a lack of robust compliance. Accordingly, crypto forensics and analytics for LEAs present significant challenges. The challenges and risks are often related to a lack of clear understanding regarding data meaning, types, compliance, ethical use and the broader efficacy of analytics tools and outputs. Operational and design risks are often further increased due to knowledge and information asymmetries relating to technological expertise, data compliance (state, trans-state and international) and general lack of ethical understanding relating to citizen data use and misuse.

Moreover, as Frows et al. [10] emphasise, cryptocurrency forensics and analytics require robust data and ethical compliance to mitigate the risk of failed prosections due to a lack of data compliance and ethical rigour in the design and use of such forensics. This challenge is most evident when considering the level of data compliance rigour and precision a judge requires to determine a prosecution while also considering potential legal challenges. Hence, for any cryptocurrency forensics solution and the inherent use of public data to offer success in terms of actionable results and value, the system logic of (i) data capture, (ii) processing, (iii) analytics and (iv) outputs must achieve data and ethical compliance through each phase of operation. AFT researchers and commercial stakeholders will operationalise this rationale in the design and development of tools. Further supports from informed use of available tools and methods that support better data and ethical compliance, and there is a potential to adapt them to specific use cases and contexts. AFT follows such a strategy of developing machine crypto forensics and intelligence solutions that process public and available data for law enforcement, but it takes a robust strategy of embedding compliance and ethics in the research community and culture of the project. Given the emphasis on this requirement for robust data compliance and ethics to mitigate potential project risks and harms, D1.3 addresses the concerns in a proactive three-pronged strategy of (a) research ethics compliance, (b) data compliance and (c) professional and ethical compliance in practice, via a code of conduct, to mitigate the risks. AFT will develop a strategy that utilises and optimes many soft governance instruments to support hard data regulation and enable a more comprehensive risk mitigation strategy. Synthesised values from data and AI compliance, governance and ethics will inform the design, development and end-use of AFT tools in order to remove and address risks of societal harms.

That said, the justification of monitoring personal data to mitigate social risks and citizen harms is at the end of a spectrum that presents an accumulation of tangible risks. There are necessarily several phases of public and personal data use that precede such a level, and the legal mechanisms, instruments and ethical

guidelines are applicable to citizens until a threshold of risk is achieved[8]. Nonetheless, temporal phases relate to any form of citizen monitoring or surveillance that also present different risk contexts and meanings. Therefore, the design of AFT tools demands an informed understanding of how temporal phases and changing risk phases along with the increased accumulation of risk changes the nature of data compliance and data ethics.

ULIM's strategy to D1.3 is to provide the necessary conceptual apparatus, scaffolding and methods to steer the data-centric operations (tool design and tool use) within the AFT project. The strategy is built upon building an AFT community with a culture of integrity and caution regarding data use. As deliverable leaders, ULIM takes a cross-discipline and cross-sector approach to capture, assess and guide data analytics operations and practices with high-risk societal relations. D1.3 utilises socio-political science research to develop a framework of principles, descriptive tools and methods as methodological insights to support more informed professional decision-making by consortium participants. Accordingly, research ethics and data science governance are combined to provide a context-specific framework of guidelines for best and responsible practices. The outputs of D1.3 provide a mechanism that researchers can access as research ethics, a code of conduct of research and a decision guide to support FAIR[9] and ethical practices.

> *"Due to a lack of discussion within the realm of data and computer scientists of these issues, it appears that public accessibility lacks a common understanding and regularly depends on individual perceptions. In the broadest manner, data may be publicly available if it is not subject to a state-of-the-art protection. For professional data scientists the scope of publicly available is hence likely to be broader than in the legal understanding - either in the US or the EU." [2]*

Hence, the challenge to support technical expertise with data compliance, governance, and ethical knowledge and skills will be operationalised in a cyclical community engagement, openness, shared assessment, and a co-auditing process. For example, as questions and challenges arise, they will be clarified and become part of the data and research logs. This process is captured in figure 1 (below) and will provide valuable information that will also be considered every quarter and used to support the AFT code of conduct development.

[8] The rights of citizens is embodied in the foundational pretext of the EU Charter of Fundamental Rights: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

[9] See: FAIR Principles - GO FAIR (go-fair.org)

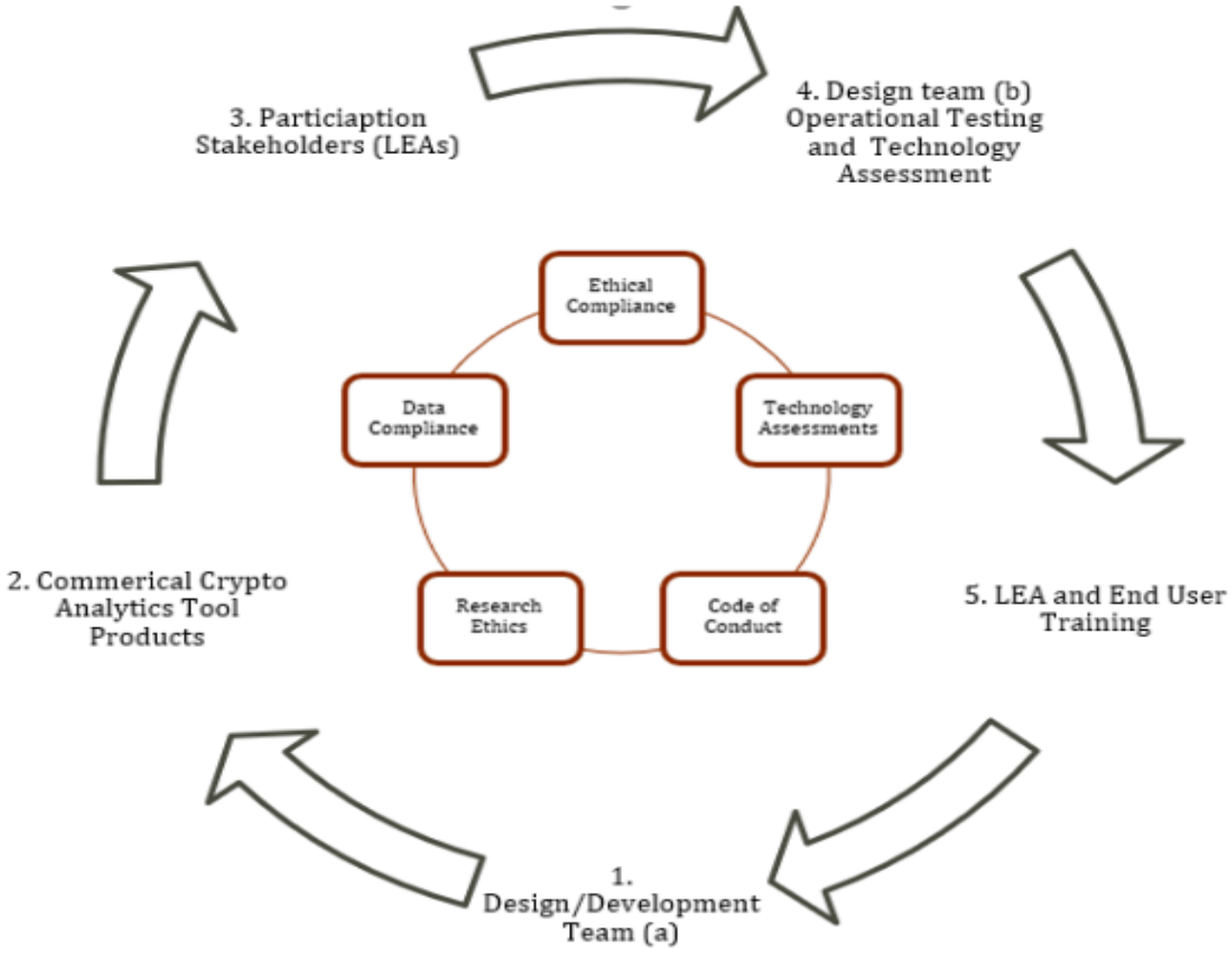

Figure 2: AFT Compliance and Ethics Process Cycle

3 Research Ethics and Anti-FinTer design and development activities

3.1 Research Ethics

Research and technological innovation are more important than ever in supporting socio-economic development as well as promoting safer societies. The Horizon program developed in the EU was innovative for many reasons, but one key innovation theme concerns how it embedded research ethics into all research funding and activities[11]. In particular, the focus on science with and for society remains fundamental to EU research and funding, and this is built upon embedded research ethics. The successful operation of research ethics is pivotal to achieving "*research excellence in all domains*" [11]. Furthermore, the EU strategy supporting Responsible Research and Innovation (RRI) is also intrinsic to EU research ethics and practices[11, 12].

The ALLEA framework is described as the "*common strategic framework for EU research and funding*" [13]. It is a European research integrity framework built upon identifying and creating a strategic response to "*professional, legal and ethical responsibilities, and acknowledges the importance of the institutional settings in which research is organised. Therefore, this Code of Conduct is relevant and applicable to publicly funded and private research, whilst acknowledging legitimate constraints in its implementation*."Accordingly, it is important to assess and support innovations that promise to mitigate societal risks. What kind of assessments and supports may depend upon the types of technologies and innovations. When citizen data, public data and sensitive data use is key to innovation and especially innovations that claim to provide social benefits, it is important to provide a robust data assessment framework. Research ethics provides a foundational start to any data governance framework because research ethics promotes design, research and practice professionalism and integrity. The foundational principles of research ethics are the first port of call to assessing and understanding potential risks to innovations. In this way, Research ethics is a pivotal tool to risk identification, communication, transparency, accountability and risk management.

3.1.1 European Code of Conduct for Research Integrity

Consortium members must comply with the requirements of the European Research Integrity as set out in the ALLEA framework. The strategy supports researchers' self-regulating in their research decisions, and the framework acts as a strategic guideline supporting best practices in a research community environment. Research communities are increasingly complex by nature of the public and private partnerships. It is sometimes the case that partners may have differing priorities and interests from research collaboration and outputs. For example, a private actor providing data analytics products and services for LEAs may have very different conceptions of what public data is that feeds into their systems and, more importantly, may see data compliance and ethics as less relevant than a judge presiding over high profile case that is built upon data use and the resulting intelligence. Therefore, guidance and research integrity provide a common language that unites research goals and activities with the broader community and societal values. In this way, codes of ethics and professional codes of conduct have become invaluable tools that operationalise ethical and value-based principles to support research autonomy while embedding core research and societal values. Like so many other codes of conduct, ALLEA takes a strategy of creating a code informed by key principles unique to the context of research. Research integrity is a necessary foundational component to all EU-funded research activities[10]. Research integrity demands the highest standards of "*professionalism and rigour*" in all activities while also operationalising research ethics into both experimentation, project outcomes and dissemination[11].

[10] See

[11] See Irish Universities Association -www.iua.ie- and Royal Irish Academy -www.ria.ie-.

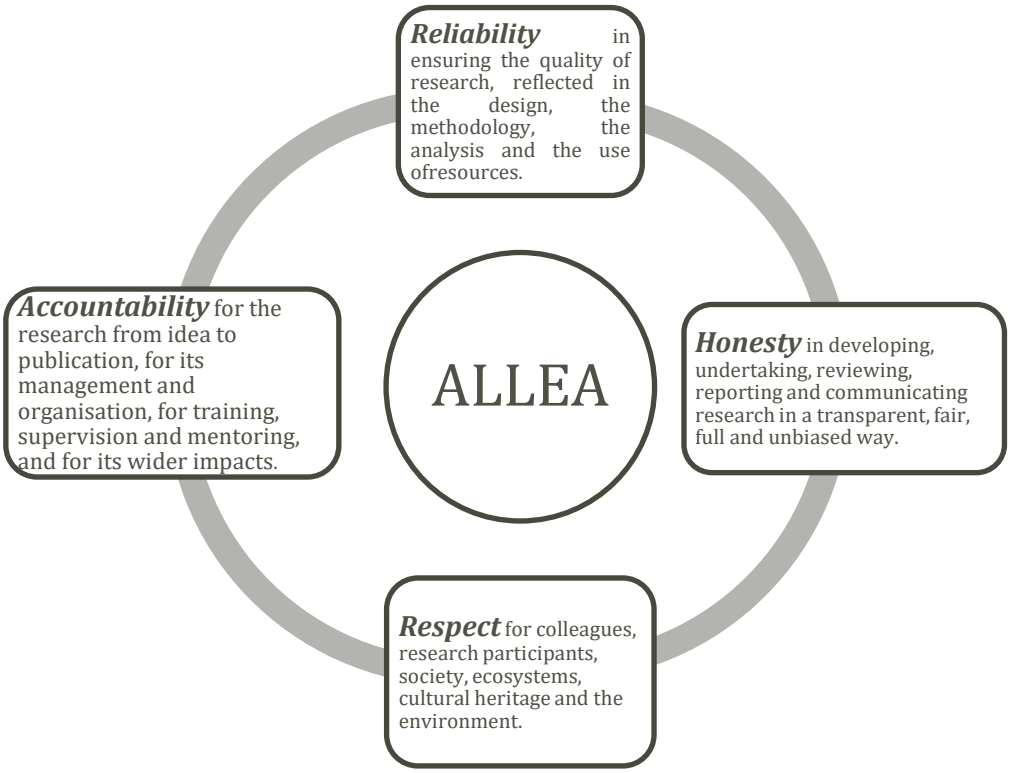

Figure 3: ALLEA Framework

In addition to ALLEA, a wide range of relevant sources focus on practical solutions to support research integrity. These range from "Research Integrity: nine ways to move from talk to walk" communicating key best practices[14] to the innovative project called SOPs4RI, which supports greater research integrity through a practical toolkit. Common ideals and principles are appealed to in order to inform the AFT research integrity strategy. Furthermore, junior researchers will be mentored throughout the project and directed to a support program such as Upright.

3.1.2 Ethical compliance supporting Research Integrity through Practice

AFT will promote and sustain a research culture built upon the ALLEA principles and Responsible Research and Innovation. All members of the research community throughout all phases and locations of research will abide by the ALLEA framework as a necessary requirement to research activities and decision-making. Therefore, AFT provides a research ethics framework that supports community integrity and professionalism. The framework is one of several layers that provide a foundation to support community integrity and value-aligned decision-making. The framework is the first step in preventing misconduct and also in providing clear guidelines that enable greater compliance and accountability. In this way, the research ethics framework acts as an initial internal policy framework emphasising professional behaviour and admonishing unprofessional behaviour.

3.1.3 Specific Risk Hotspots and Counter Measures

The focus on strategic operationalisation of research integrity and ethics guidelines has practical utility by stimulating a culture that aims to mitigate the risk of research misconduct through informed decision-making and practice. In this way, the EU strategy emphasises the need for multiple preventative approaches to avoid misconduct.

AFT is a data-focused research project and accordingly takes progressive actions to operationalise a robust regime of data management and governance. To support the ALLEA framework's focus on responsible use of data in research activities, AFT will utilise a digital evidence management framework as part of the research ethics and data governance strategy.

AFT will operationalise research across several locations and will co-ordinate with all researchers as a coherent and united research community complying with a common charter of research ethics and data management.

Each internal group will identify a research ethics and data compliance officer to oversee and sustain the necessary organisational structures.

Each research context and use of data will identify its own unique research risk table along with the appropriate safeguards and risk mitigation procedures.

In quaterly cycles AFT stakeholders will meet to assess and update the AFT code of conduct for design and use.

3.1.4 Operationalising Safeguards and preventing Misconduct and Misuse

Following the work from Titanium and its emphasis on the need for a robust user safe-conduct framework, AFT adopts the same rationale that emphasises the need for further authentication to access pseudonymisation. The option of pseudonymisation is only available to standard users when a threshold is reached. A threshold could consist of accumulating several risk flags, which justifies access to pseudonymisation options otherwise unavailable.

1. **AFT** will adopt the robust EU program for research ethics and its ALLEA framework as the foundation of practice and operations.

2. **AFT** will adopt a policy of data contextualisation, minimisation and proportionality in its data gathering and processing activities.

3. **AFT** should employ a policy of caution to all data retrieval and use it to counter the uncertainty and knowledge gaps commonly associated with design engineers and end-users regarding sufficient in-depth understanding of data compliance.

4. **AFT** will employ a modus operandi of caution regarding all data regarding retrieval, processing, analytics, insights and storage.

5. **AFT** should develop a filtering solution that can provide access and monitoring of justified profiles and not impede the rights and privacy of law-abiding citizens.

6. **AFT** will support transparency in design and use in terms of a superficial disclosure of non-sensitive and non-classified operational goals, risks and risk mitigation strategies.

7. **AFT** operationalises an Ethics Advisory Board to support the operationality of the research ethics framework, data management and compliance and addressing any emergent risks or concerns.

8. **AFT** will include key stakeholders from LEAs with field labs and training events to promote community engagement and participation in the research code and in the operational code.

9. **AFT** will develop a context-specific code of conduct for the safe, compliant and ethical use of the tools. The code of conduct will be, where required, further supplemented by a guidebook concerning risk communication and mitigation.

4 Guiding Ethical Analysis of Anti-FinTer Tools and Services

4.1 Data Governance and Compliance (baseline)

Crypto forensics and analytics often use data analytics techniques to create an identifiable pattern that can act as a profile. The pattern acts as a placeholder (identifier) profile for a targeted entity. Two techniques are commonly used to achieve this; (a) clustering heuristics (grouping of data points (values) such as addresses in a relational pattern to provide unique identifiers for an entity or person) and (b) attribution tags (which consist of a catalogue of secondary information that supplements the information profile of (a)). This complex technical strategy may provide important benefits to LEAs and other state actors responsible for mitigating the risk of criminal behaviour, but for such innovative strategies to provide actionable insights and value, the design and use of such innovations must be sufficiently robust that the insights and actions are both legal and ethical. Accordingly, to achieve such legal and ethical rigour, a robust strategy of research ethics, data compliance and ethical analysis is required to inform the design and use of any data analytics strategy for LEAs.

To achieve the required legal and ethical rigour to support trustworthy and compliant actions from AFT tools, D1.3 focuses on developing a strategy of data and ethical compliance empowerment for all stakeholders within the AFT development pipeline and also in the community of end-users that will operationalise the tools.

The complexity of research, especially research that involves data analytics concerning EU citizen data, means there are always rules in place regarding what are acceptable research practices. Compliance is a powerful conceptualisation because it sets out clear parameters for what is and is not acceptable. That said, recent decades have brought about a dramatic change in technologies and especially data centred innovations. Regulatory instruments such as the GDPR (General Data Protection Regulation) often means that researchers can appeal to regulation to support more informed research decisions regarding personal data. Moreover, with the EU's other data centred Acts such as the Data Governance Act (2020), Digital Services Act and Digital Markets Act (2021) and the emerging Data Act (2022), a great deal of specific guidance is available. Consequently, the GDPR provides a hard law and hard governance mechanism policed and enforced by each state's data commission. Accordingly, European data is protected by a robust regulatory regime, and significant fines can follow where actors have failed to comply with the specifics of the GDPR.

The EU has created a robust data governance strategy and operationalised several data governance mechanisms and instruments to steer data research, innovation and commercialisation. The catalogue of mechanisms and instruments provide data governance scaffolding upon which data practices can be built with an awareness of clear and transparent regulatory compliance. However, even the most robust data regulation as enacted in the EU can only provide so much guidance and utility. The complex and fast-paced nature of data and AI innovation means that regulatory instruments can soon lose traction in capturing state of the art and emerging innovation operations and practices. Accordingly, grey areas and gaps are common, and this means that social values, ethical values and professional values are operationalised in softer forms of governance such as research ethics, codes of conduct and professional charters. A common theme throughout data and AI governance regimes are to access governance value in informed ethical and professional decision making.

Therefore, the AFT strategy is to develop and operationalise three strategic pillars that provide descriptive and prescriptive support to stakeholders within the developmental pipeline. The first concerns research ethics and professionalism in the European Charter (ref). The second concerns compliance with the EU's data governance regime and the many mechanisms and instruments. The third concern addresses the spaces and decision contexts that are not captured by research ethics and data/AI compliance. Hence, the third build a

context-specific code of professional code to further support the design decision making of AFT tools and the use of the tools by stakeholders.

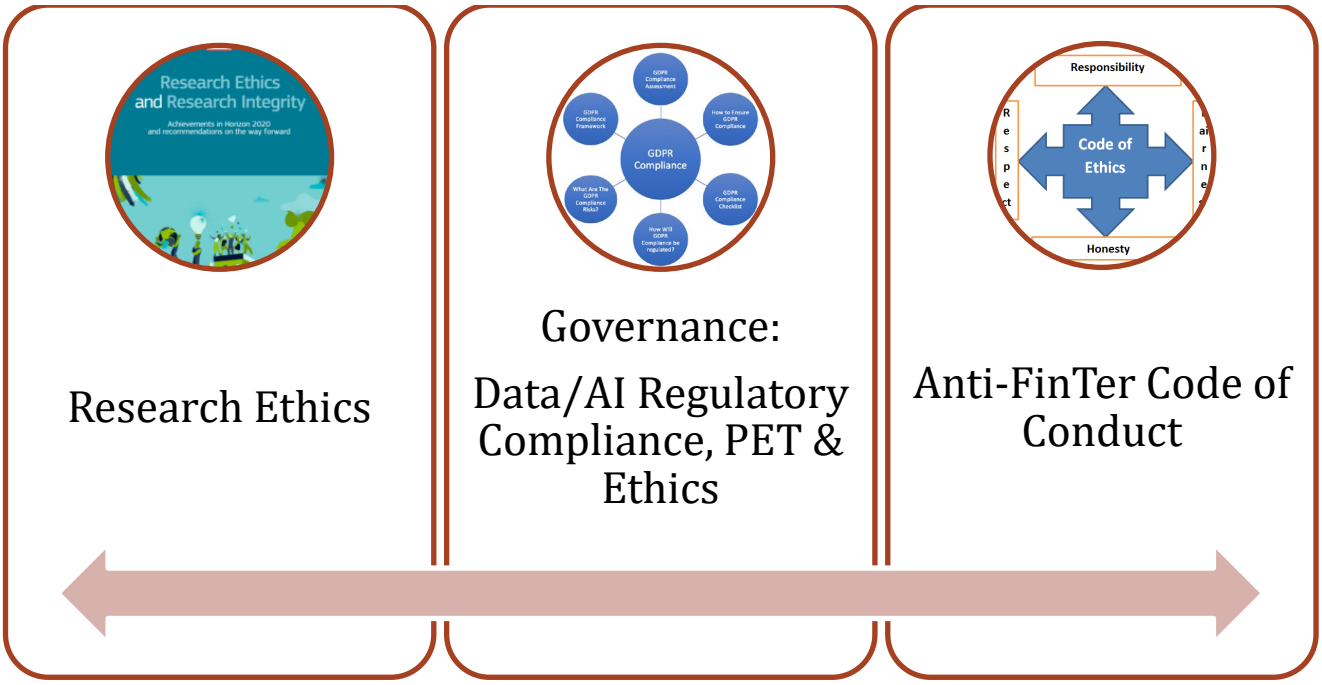

Figure 4: AFT operational Pillars

4.2 Professionalism

4.2.1 Research Team

Data and AI-centred research demand a unique skillset of programmers, developers and engineers working in teams to design and develop unique solutions. EU data compliance demands that within such teams, key roles of responsibility and accountability are operationalised to manage and steer activities toward positive outcomes while also identifying and managing risks.

4.3 Data Governance Mechanisms and Instruments

4.3.1 Core Ethical Principles

Principlism has proven to be a helpful mechanism for applied ethics in technological contexts of innovation. Professor Luciano Floridi [15-17] has adapted Principlism as developed by Beauchamps and Childress[18, 19] specifically to contexts of data and AI. Accordingly, Principlism, specifically Floridi's version, is utilised as the core ethical instrument to inform and guide AFT tool design decision-making. Principlism and the principles are acute in capturing a range of moral norms in an accessible and practical format. Accordingly, AFT uses a strategy of ethics by design to embed ethical principles and positive engagement to inform the design and use of the tools. A positive outcome of this action concerns reducing the downstream ethical risks of misuse and the burden of ethical deliberation on end-users and stakeholders, which is achieved by actively supporting the moral development of the research team and enabling a community of support to participate in ethical decision making. Therefore, this approach to embedding ethics and operationalising ethics by design offers important utility in determining outputs that are more value-aligned, safer and introduce less immediate and downstream operational risks. For example, justice speaks to the ideal of fairness most acutely in the distribution of benefits and risks. Accordingly, such fairness demands a foundation of equality in engaging and dealing with citizens and groups. It is important to ensure that no citizen or group is

disproportionally targeted by the tools. The risk of algorithmic bias is also a factor here, and this risk identifies a risk of unfairness and significant power imbalances created from the design and use of soft surveillance tools.

- Autonomy

  Respect for citizens' right to choose their own actions and have the capacity for self-determination. In AFT, Autonomy has several dimensions that range from its intrinsic value to data consent, use and transparency.

- Beneficence

  To pursue human and societal good as the primary value of research and design decisions and actions. In the context of data and analytics of public data, this could also translate as more significant consideration and care for how citizen and public data are used for enterprise.

- Non-maleficence

  A core maxim concerning the primary principle of 'first do no harm. The guiding ethos is that all researchers should be informed by a requirement to do no harm to colleagues or other stakeholders through their actions or inactions.

- Justice

  Societies present different risks, and resource distribution is key to responding to many forms of risk. Hence, AFT functions could introduce resource management questions in responding to significant risk scenarios.

- Explicability

  The relatively new framing of ‘explicability’ is key to data use because it demands a fusion of explainability and accountability

4.4 Data Compliance, Privacy Enhancing Technologies and Ethics by Design

4.4.1 Data Provenance

Data management is fixed into the operations of any data enterprise because it secures control, value and safety. Data provenance is a further layer of supporting data compliance, and it acts as a form of robust self-governance. Data provenance enable a common data risk management architecture to develop in parallel with operationality and changing dynamics. In this way, data provenance is an invaluable and economic strategy to secure data compliance and additionally provides significant further risk management opportunities.

4.4.2 Privacy by Design

The design and development of AFT tools present challenges to designers in terms of making informed decisions that are compliant with data regulation. Moreover, designers increasingly have a duty to ensure their decisions are informed by at least an awareness of ethical questions, tensions and considerations. Where data is used, especially where public and personal data is used, there are often ethical relations to the use of data. Ethics provides an important lens to support a better understanding of the impacts of research and innovation. In the EU, Responsible Research and Innovation has become a foundational theme to supporting research and innovation that aligns with EU societal values [12]. Data scraping and analytics for commercial enterprises, even in the use case of LEAs, must still respect privacy. Moreover, there are already

tools and methods that support privacy by design in developing data analytics tools[12].Accordingly, AFT will assess and implement a wide range of privacy by design methods to support research integrity.

4.4.3 Ethics by Design

4.4.3.1 Accountability

Accountability is key to project operations and successful outcomes because it embeds a community duty of care and responsibility. Moreover, accountability offers a construct that supports greater quality and assessment in operational practices. Accountability is also intrinsic to securing causal chains of responsiility regaridng decisions and actions. With regard to data, the data provenance strategy supports greater accountability.

4.4.3.2 Proportionality

Who weighs the proportionality of data use and social risk mitigation in the context of data and crypto forensics tools is an important question. The design of any artefact should be informed by any ethical tensions and the necessary analysis to reduce the downstream ethical burden. Hence, proportionality by design is a necessary value-added component to the AFT system and operations. A risk to any data forensics tools for LEAs and other actors concerns what Koops et al. refer to as "*notions of mission creep, competence creep, and authority creep.*"[13]

[12] See Fovino, Igor Nai, Marcelo Masera, Privacy Preserving Data Mining, Evaluation Methodologies, JRC Scientific and Technical Reports, JRC JRC42699, EUR 23069 EN, 2008; US Department of Homeland Security, Privacy Policy Guidance Memorandum, Memorandum number 2008-01, 29 December 2008, p. 3-4.
https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

[13] See one of the seminal works relating to 'Function Creep' by Winner, Langdon, *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought*, The MIT Press, Cambridge, MA, 1978, p. 244.

5 Development of an Anti-FinTer Code of Conduct

5.1 Operationalising Compliance and Ethics in a Context-specific Code of Conduct

Cross-state deployment of data-centric tools such as AFT that target financial fraud across many states provide important strategic risk mitigation benefits. Targeted analytics of dark web and crypto transactions is key to intelligence-gathering for criminal and terrorist risk mitigation. That said, the development, design and deployment of such data-centred technologies also introduce their own unique set of risks. Operational risks relating to the use of personal and sensitive data such as citizen and institution financial data requires compliance with robust regulatory mechanisms such as the GDPR (2018), the EU Markets and Services Act (2021), and other existing and emerging instruments such as Data Act (2022). The GDPR replaced the Data Protection Directive 1995/46 by providing a more informed and robust response to digital and data centred innovation. The GDPR takes a more robust three-pronged approach to data governance by specifying compliance in terms of data type (personal data, industrial data, sensitive data), management (storage and processing of data) and movement (transfer of data)[14]. Data compliance is an essential component of any data-centred approach and requires adherence to a range of aspects supporting compliant activities and operations. That said, the GDPR and other instruments will often only go so far in providing clear guidelines to inform decision-making and operational activities. Accordingly, it is often necessary to develop supporting strategies to provide further assistance and guidelines to stakeholders using citizen data. As data and AI applications push innovation forward, compliance and regulatory mechanisms can soon become outdated and less effective in guiding data professionals and practitioners in making informed research and data use decisions. Accordingly, many data analytics development pipelines and data' use' strategies adopt soft governance instruments such as specific codes of practice, research and ethics to support professionals and the products and services they design and create.

Professional bodies and practitioners have strategically used codes of conduct as a form of self-regulation to guide professional behaviour for decades (Medicine and healthcare, Engineering [15], Computing [16]). Professionals using big data analytics, AI and ML have a less contextual understanding of the utility and supporting benefits of a code of professional conduct. That said, big technology actors have, in some scenarios, utilised codes of conduct to support commercial operations, decision-making and value alignment strategically. Microsoft[17], Google and Facebook have all developed robust codes of conduct. Furthermore, developing a code of conduct requires a community of engagement and participation to support operationality, otherwise, it may not offer any significant governance benefits. Hence, a code of conduct requires critical assessment and community participation to optimise the code in terms of operational value.

[14] See: ""Personal data" is any information that relates to an identified or identifiable living individual (data subject) such as a name, email address, tax ID number, online identifier, etc. "Processing" data includes actions such as collecting, recording, storing and transferring data." European Union - Data Privacy and Protection | Privacy Shield

[15] Engineers Australia, Engineers Ireland

[16] ACM

[17] Microsoft Code of Conduct

5.2 Supporting Operationalisation: Self Assessment and project Auditing

The AFT community promotes a culture of openness and transparency regarding research within the project. Furthermore, open knowledge and knowledge-sharing is paramount to enabling not just transparency but also internal auditing and self-assessment.

5.2.1 Sustaining a Professional Community

Developing a professional community of practice requires compliance with laws, rules, regulations, soft governance instruments such as organisational principles and charters, as well as ethical understanding. A professional community should also be an ethical community that shares common values of trust, accountability, transparency and care. It is an important part of any bottom-up governance for communities.

However, an over-reliance on rewards and punishments does not lead to more ethical behaviour (McDonald, 2009). Instead, the Code of conduct should guide and support more informed decision making by sustaining the moral objectives of the community. A positive ethical environment community is foundational to stronger ethical decision-making (McDonald, 2009) in the face of uncertainty and dilemmas. Informed decision making transforms risk to governance value during key decision-making opportunities within the engineering or scientific design process. McDonald (2009) proposes the following as six universal moral values present with Codes of Ethics:

1. Trustworthiness
2. Respect
3. Responsibility
4. Fairness
5. Caring
6. Citizenship

McDonald's approach further validates the work of Beauchamp and Childress as well as Floridi's updated and technogy specific application.

1. Beneficence
2. Non-Maleficence
3. Autonomy
4. Justice
5. Explicability

To optimise the potential benefits of a code of conduct it is necessary to create a context-specific code informed by principles thhe moral and value complexity and most imprtantly provides supports in proactively responding to moral and value complexity and uncertainty.

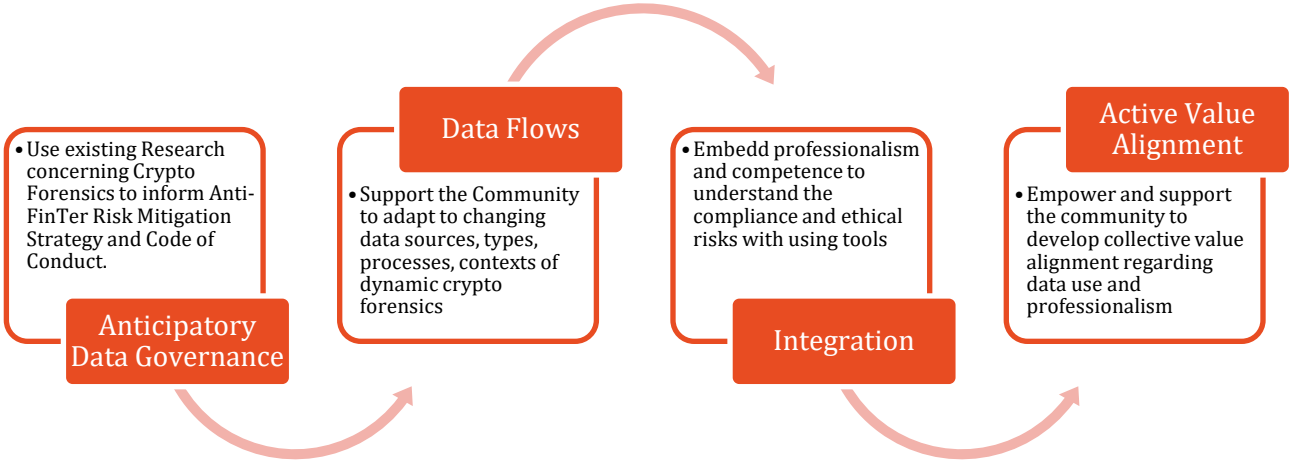

Figure 5: AFT Governance Flow

5.3 Anti-FinTer Code of Conduct

AFT suite of tools and methods are designed to provide decision support intelligence to LEAs and other agencies. Due to the unique nature of the data sources, processing and outputs that could determine high-risk actions, it is necessary that users of the tools are supported in responding to scenarios where there may be identifiable concerns, value conflicts and ethical tensions regarding the insights provided by tools. In this way, the operations manager and end-user must complete a data forensics readiness assessment that communicates some of the data and ethical management contexts that the use involves.

1. Data: Data Flows, Insights and Risk
AFT tools are supported by a robust foundation of research ethics, Privacy-Enhancing Technologies and data ethics audits and assessments. That said, risks will remain, and the community must be cautious. This is because of the high-risk data context that comes with crypto forensics. In short, even the most compliant and ethically robust data management strategy will not provide complete risk mitigation, and some risks will remain. Hence, operational and section managers supporting end-users must be cognizant of the potential risks and acknowledge with the community that the nature of the data sources, the context of data use and the intelligent solutions that provide the functionality to gain outputs means that all use comes with a caution.

2. Data Responsibility
To mitigate some of the risks relating to the use of AFT tools, operational managers and end-users offer the most value. Responsibility and awareness are intrinsic to mitigating the risks of harm by normalising caution relating to results and promoting a culture of use that supports questioning results and potential outcomes.

3. Data Accountability
A digital user agreement needs to be signed with each use context of operation, and this is part of the digital evidence management framework supporting data provenance. In addition, with the user log all actions carried out by the user are recorded and saved securely for a period of four years. A period of four years is necessary to comply with the possibility of appeals.

4. Responsible Use

The use of commercial products and services to support LEAs and their operations is common, but the relatively recent move to the use of commercial services built upon scraping public data and providing an analytics solution introduces new complexities to public/private relations. Some of the complexities related to risk and ethics. In particular, questions of data ownership, access and monitoring the use of commercial analytics tools by end-users creates a complex risk scenario. AFT appeals to the work of past projects to promote a strategy of responsible use of analytics and forensics tools. All users must comply with the commercial actor's terms of service agreements and, where possible, the specific codes of conduct provided by commercial actors that are specific to their products and services.

6 Conclusions

AFT is an innovative project that presents significant opportunities to identify present and emerging socio-economic risks relating to the criminal use of cryptocurrencies. In particular, the high-risk scenario of terrorist financing presents a risk scenario that continues to impact the EU. Accordingly, AFT addresses not only the technological innovation challenges and risks but also the more societal, legal and ethical relations, tensions and challenges. Both aspects present a catalogue of risks that threaten to undermine and limit the potential benefits of AFT. Therefore, D1.3 confronts this challenge as an opportunity to provide a robust strategy of support to AFT, its research community and its stakeholders and end-users. The three pillars of D1.3 provide a sophisticated multilayered and dynamic response to support, manage and mitigate the wide range of risks that parallel the development and use of AFT tools. In this way, D1.3 provides a hybrid response that captures research communities' top-down, bureaucratic and bottom-up drivers to enable professionalism, trustworthiness and research, all of these sustains the core foundation of responsible research and innovation for societal benefits while respecting societal values. EU LEAs can benefit from data and analytics intelligence solutions by becoming responsible and active participants in the EU strategy for collaborative data spaces.

Bibliography

1. Lotfi, M., et al., *Transition toward blockchain-based electricity trading markets*, in *Blockchain-based Smart Grids*. 2020, Elsevier. p. 43-59.
2. Gottschalk, T., *The Data-Laundromat? Public-Private-Partnerships and Publicly Available Data in the Area of Law Enforcement.* Eur. Data Prot. L. Rev., 2020. **6**: p. 21.
3. Nieto, A., et al., *Privacy-aware digital forensics*. 2019.
4. Hale-Ross, S., *The UK's Legal Response to Terrorist Communication in the 21 st Century: Striking the Right Balance between Individual Privacy and Collective Security in the Digital Age*. 2017: Liverpool John Moores University (United Kingdom).
5. Hale-Ross, S., *Digital Privacy, Terrorism and Law Enforcement: The UK's Response to Terrorist Communication*. 2018: Routledge.
6. Meghanathan, N., S.R. Allam, and L.A. Moore, *Tools and techniques for network forensics.* arXiv preprint arXiv:1004.0570, 2010.
7. Cosic, J. and M. Baca. *Do we have full control over integrity in digital evidence life cycle?* in *Proceedings of the ITI 2010, 32nd International Conference on Information Technology Interfaces*. 2010. IEEE.
8. Bača, M., J. Ćosić, and P. Grd. *Using DEMF in process of collecting volatile digital evidence*. in *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 2016.
9. Chandramouli, K., et al., *MAGNETO D5. 3-Court-proof Forensic Evidence Toolset.* 2020.
10. Fröwis, M., et al., *Safeguarding the evidential value of forensic cryptocurrency investigations.* Forensic Science International: Digital Investigation, 2020. **33**: p. 200902.
11. Commission, E., et al., *Research ethics and research integrity : achievements in Horizon 2020 and recommendations on the way forward*, ed. N. Delaney and Z. Tornasi. 2020: Publications Office.
12. Commission, E., et al., *Responsible research and innovation (RRI), science and technology : report*. 2013: Publications Office.
13. Engelbrecht, J., N. Mann, and J.J. Schroots, *ALLEA-is the Federation of 53 Academies of Arts and Sciences in 42 European countries ALLEA-advises her member academies, acts as a platform for her members and offers advises in the fields of science and science policy ALLEA-strongly supports ethic ways of dealing with science, science.*
14. Mejlgaard, N., et al., *Research integrity: nine ways to move from talk to walk*. 2020, Nature Publishing Group.
15. Mittelstadt, B.D., et al., *The ethics of algorithms: Mapping the debate.* Big Data and Society, 2016.
16. Floridi, L., et al., *AI4People-An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations.* Minds Mach (Dordr), 2018. **28**(4): p. 689-707.
17. Floridi, L., *Soft Ethics and the Governance of the Digital.* Philosophy & Technology, 2018. **31**(1): p. 1-8.
18. Beauchamp, T.L. and J.F. Childress, *Principles of biomedical ethics*. 2001: Oxford University Press, USA.
19. Beauchamp, T.L. and J.F. Childress, *Response to Commentaries.* The Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine, 2020. **45**(4-5): p. 560-579.

6.1 Referenced Documents

Three EU Horizon 2020 projects are directly relevant to Anti-FinTer. Indeed the research outputs and insights from these projects have provided an important foundation to build upon. In particular, the Societal, ethical and Legal contexts of crypto forensics are considered in some depth throughout these projects.

ASGARD

TITANIUM

TRUST

Section One: Challenge Space Data Risk, Ethics and Governance

Harrigan, Martin, and **Fretter, Christoph**, The Unreasonable Effectiveness of Address Clustering, http://arxiv.org/pdf/1605.06369v2*, accessed 16 April 2018*.

Section Two: Research Ethics

European Commission, European Textbook on Ethics in Research, Luxembourg, 2010. https://ec.europa.eu/research/science-society/document_library/pdf_06/textbook-on-ethics-report_en.pdf

European Commission, *Research, Risk-Benefit Analyses and Ethical Issues: A guidance document for researchers complying with requests from the European Commission Ethics Reviews*, 2013. https://ec.europa.eu/research/swafs/pdf/pub_research_ethics/KI3213113ENC.pdf

The European Parliament, the Council and the Commission, Charter of Fundamental Rights of the European Union, 2000/C 364/01.

Section Three: Legal, Governance and Compliance

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation,
Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP 258.
Peers, Steve (ed.), The EU charter of fundamental rights: *A commentary* (Hart, Oxford: 2014).

The European Parliament and the Council, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), L 119/1.

The European Parliament, the Council and the Commission, Charter of Fundamental Rights of the European Union, 2000/C 364/01.

Section Four:
Mcdonald, G. M. (2009). An anthology of codes of ethics. *European Business Review*.