TOWARDS A SOCIALLY ACCEPTED AND SUSTAINABLE 6G

November 2025

Policy Brief on Safeguarding Privacy in 6G

Carmela Occhipinti
Tetiana Vasylieva

6G4SOCIETY

CyberSocial Lab.

1. Highlights

Europe's transition toward sixth-generation (6G) mobile network will significantly intensify data collection, as billions of connected humans, devices and digital twins generate continuous and often invisible streams of personal and behavioural information. Citizens already identify privacy as their primary concern for future connectivity, expressing deep concern about surveillance, loss of control, and opaque AI-driven decision-making. Project findings confirm that existing EU privacy and data-protection frameworks, while robust, were not designed for 6G's hyper-connected, distributed and globally interdependent architecture, leaving gaps in user control, profiling governance, accountability, and cross-border safeguards.

Evidence gathered through citizen surveys, expert and policy makers interviews, and Smart Networks and Services Joint Undertaking (SNS JU) project analysis points to five priority risks: erosion of user agency, foreign access to EU data, discriminatory or opaque AI decisions, unclear responsibility across multi-vendor networks, structural tensions among stakeholders with diverging privacy interests, sensing and geolocalisation, privacy and security. These insights underscore that the success of 6G will depend not only on technological progress but on embedding European values such as privacy, fairness, accountability, and sovereignty into its governance and design.

Against this backdrop, this policy brief examines the central question:

HOW CAN EUROPE SAFEGUARD PRIVACY AND FUNDAMENTAL RIGHTS AS 6G NETWORKS BECOME MORE DATA-INTENSIVE, AI-NATIVE, DECENTRALISED, AND RELIANT ON GLOBAL SUPPLY CHAINS?

It proposes six main recommendations:

1. Restore user control over 6G data processing
2. Protect EU data sovereignty from cross-border and foreign access risks
3. Regulate AI-driven profiling and automated decisions
4. Clarify accountability across complex 6G ecosystems
5. Reconcile conflicting privacy interests within the value chain
6. Modernise legal rules for location data
7. Enforce privacy, data protection and security literacy
8. Reinforce targeted research and coordinated policy support

2.Context of the Issue

As 6G will bring together humans with massive instances of IoT, robots, and digital twins, enabling continuous environmental sensing, and a dense web of vendors and service providers, all multiplying the personal and behavioural data that can be collected, often automatically and invisibly, policy makers and privacy authorities should be prepared. Although the EU has a robust framework for privacy and data protection including, inter alia, the GDPR, the ePrivacy Directive, the Data Act, and the Cyber Resilience Act, gaps remain. This brief supports policymakers in the implementation of the GDPR, the AI Act, and the EU's wider digital governance agenda (including the Digital Decade targets) by identifying where additional guidance, safeguards, or governance mechanisms will be needed to ensure privacy-preserving and socially acceptable 6G deployment.

In this context, the technical architecture of 6G reshapes data flows and responsibilities introducing a series of specific risks. As defined by the EDPS highlights in blog [1], 5G/6G create environments of continuous, invisible data collection, reducing meaningful consent and control. Such pervasive and invisible data flows risk **eroding personal autonomy**, as individuals **lose track of who** holds their information and for what purpose. Existing models of **consent and control are unlikely to remain effective** when data circulates across countless devices and providers. Current mechanisms for exercising GDPR rights in telecom systems are **fragmented, inconsistent, and difficult to use**. Without transparent and accessible tools that allow people to understand and manage their data, both **individual agency and accountability** will be undermined. In addition, individuals may find it harder than ever to understand **who processes their data,** especially when parts of the value chain operate **outside the EU,** raising concerns over data sovereignty and the exposure of EU citizens' information to foreign jurisdictions.

Although the GDPR mechanisms for international data transfers, as well as the EDPB recent guidelines [2] on the requirements for recognising judgments or decisions from third country on personal data transfers, **enforcement of those mechanisms** remains difficult. Moreover, although examples like the joint commitment outlined in [3] to promote trusted technologies that protect national security and individual privacy, and to advance global standards through open, transparent, and consensus-based processes supported by international cooperation, **a sector-specific arrangement** (such as an adequacy decision tailored to telecom data exchange) has yet to be established. In some cases, 6G networks bring fundamentally new privacy challenges rather than simply extending those of 5G, and existing **policies were not designed with 6G's** highly distributed architecture or its pervasive sensing capabilities in mind. For example, although 6G will be AI-native, enabling networks to make autonomous, real-time decisions about users and resources, and raising concerns about automated processing and bias, enforcement of GDPR provisions such as Article 22 on **profiling** and **automated decision-making remains uneven in the telecoms sector.**

According to [4], automated decision-making and profiling may pose risks to individuals' rights and freedoms, including the possibility of unfair or discriminatory effects and reduced transparency, which can make it difficult for individuals to understand the reasoning behind such decisions and to exercise their GDPR rights. Likewise, current rules provide limited clarity on **how profiling restrictions apply** to large-scale telecom analytics or algorithmic network management, where users might be prioritised or deprioritised without their knowledge.

Moreover, integrated sensing and communication will allow **centimetre-level positioning** and **passive environmental monitoring**, creating the possibility of continuous ambient **surveillance**.

Insights from recent project activities highlight several shortcomings in the current policy landscape. There is **no sector-specific regulation tailored to next-generation telecommunications**, and the overlapping frameworks that do exist often **lack coherence**.

This fragmentation increases **accountability challenges**, particularly when multiple vendors handle different components of the same data flow. ENISA guidelines [5] [6] stress the need for supplier risk assessments and clear governance. As outlined [7], there is a concrete risk of unclear responsibility for privacy compliance (who is the controller, who must respond to breaches, etc.). Furthermore, **competing interests** in the 6G value chain (from operators seeking to monetise data, to advertisers demanding greater access, to governments seeking data for law-enforcement purposes) risk creating structural imbalances that undermine fairness and digital autonomy.

Furthermore, while ENISA [8] underlines the importance of a common approach to telecom security for the Digital Single Market, different 6G stakeholders might have conflicting goals. **Competing interests** in the 6G value chain (from operators seeking to monetise data, to advertisers demanding greater access, to governments seeking data for law-enforcement purposes) risk creating structural imbalances that undermine fairness and digital autonomy.

3. Policy Recommendations

R1

Restore user control over 6G data processing

Ensuring that individuals can meaningfully control their personal data in 6G environments is fundamental to maintaining trust in next-generation connectivity. Strengthening user-centric mechanisms across the ecosystem would prevent situations in which people lose control over their information or cannot effectively exercise their rights, addressing the structural imbalances created by pervasive sensing and fragmented data flows. Enhancing transparency and accessible rights-management tools also aligns 6G with EU principles of fairness, autonomy and accountability, ensuring that individuals understand how their data is handled and can act on that understanding without disproportionate effort. At the same time, clear and harmonised standards providing requirements for user controls would provide legal and operational certainty to telecom operators and service providers, allowing them to implement consistent, compliant interfaces for access, consent and redress throughout complex multi-vendor infrastructures. Together, these measures shape a 6G ecosystem that preserves user agency and upholds the EU's commitment to rights-preserving digital innovation.

- Create **EU-mandated personal data spaces** for telecom/6G data. **Standardise** interoperable tools allowing users to aggregate and manage permissions for all their 6G-related data.
- Improve GDPR enforcement in telecom contexts introducing **mandatory data controller labelling** for IoT and 6G devices. Mandate physical or digital labels identifying the controller and offering **simple opt-out mechanisms,** e.g., through codes of conduct.
- Support **collective redress mechanisms** for telecom data rights. **Empower consumer organisations** to exercise rights on behalf of groups of users.
- Conduct an EU-wide public **education campaign** on 6G data practices. Provide **transparency** on what data networks collect and how users can manage settings.

R2 Protect EU data sovereignty from cross-border and foreign access risks

Strengthening robust safeguards for cross-border data transfers in 6G prevents the **exposure of EU citizens' data** to foreign surveillance regimes, reducing the risk that sensitive information may be accessed or exploited under legal systems that do not meet EU stand-ards. At the same time, it supports **European strategic autonomy** and reinforces core **sovereignty** principles, en-suring that the EU sets the conditions under which personal and operational data may circulate.

- Negotiate **telecom-specific international data-exchange agreements.** Embed privacy protections, redress, and auditability in digital partnerships and trade agreements.
- Create **telecom-specific Standard Contractual Clauses** (SCCs). European Telecommunications Network Operators should draft SCC addenda for typical 6G data flows.
- Restrict **high-risk vendors** in data-rich network segments. Build on the 5G Toolbox approach of excluding suppliers subject to foreign interference laws.
- Keep **EU data in the EU whenever possible,** and when not, apply **encryption** and legal **safeguards** when data must transit outside the EU.

Recommended policy

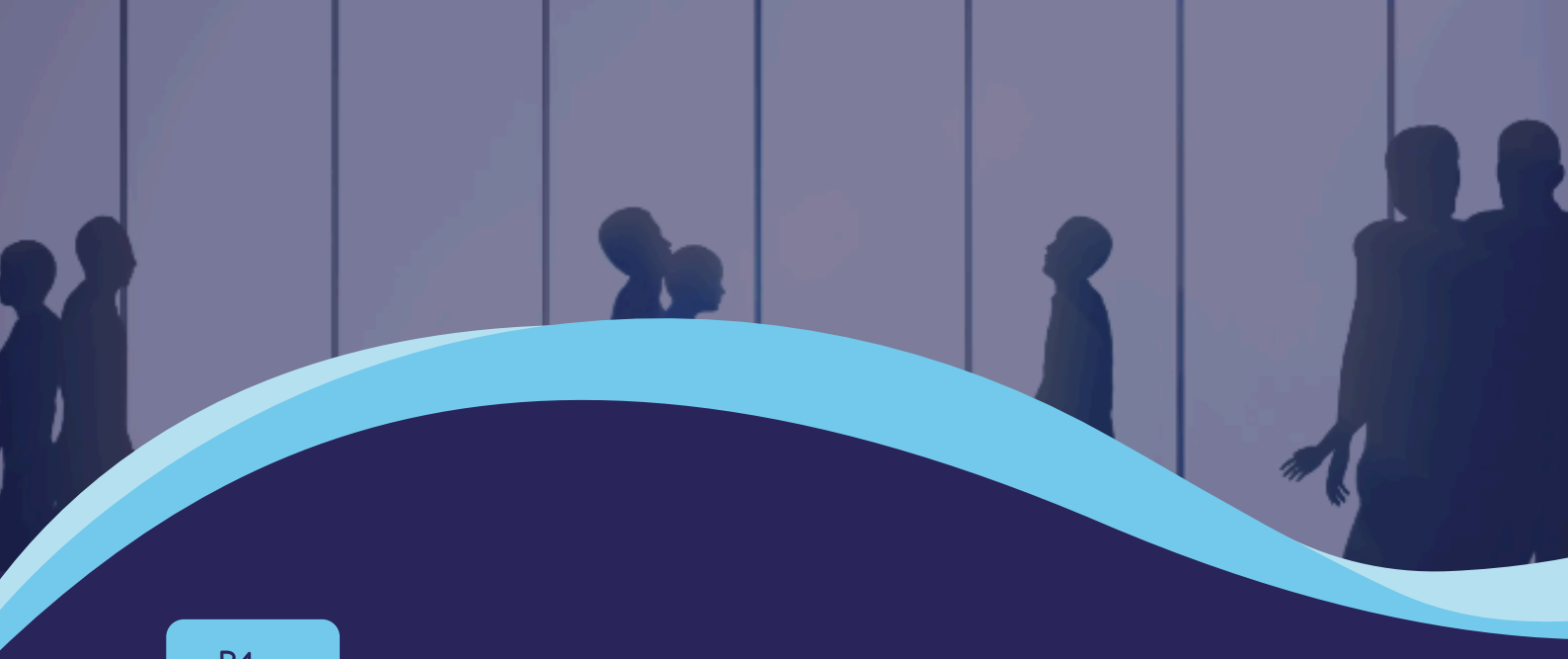
R3 Regulate AI-driven profiling and automated decisions

As 6G networks become AI-native, relying on autonomous optimisation, large-scale behavioural analytics and zero-touch network and service management, **the governance of AI-driven profiling and automated decisions becomes an immediate regulatory and compliance challenge.** In this context, AI systems embedded in 6G infrastructures are not merely consumer-facing applications, but core components of critical digital infrastructure, with direct implications for fundamental rights, fairness, accountability and public trust. Strengthening the regulation of profiling and automated decision-making is therefore essential to **prevent discriminatory network behaviour, opaque prioritisation practices, and unchallengeable outcomes affecting users and non-users** alike. These risks extend beyond individual consumer profiling to systemic effects arising from automated resource allocation, mobility prediction, quality-of-service differentiation and behavioural inference performed at network level. At the same time, the deployment of AI-native, zero-touch network management creates a **structural tension with existing legal requirements** particularly for human oversight.

Under the EU AI Act, many AI systems used in 6G network management are likely to fall within high-risk categories (Annex III), triggering binding obligations, including the requirement for effective human oversight (Article 14). However, real-time human intervention in sub-millisecond network operations is technically infeasible and incompatible with network performance guarantees.

- Issue **EDPB and AI Act-aligned guidelines** on telecom AI-driven profiling and automated decision-making. Clarify lawful bases, limits, and expectations for profiling via network-derived behavioural patterns.
- Define **sector-specific rules** e.g., prohibiting sensitive inferences on health, religion, political views from telecom-derived data.
- Explicitly recognise **AI-driven 6G network management systems as high-risk AI where applicable.** Provide guidance on how **Annex III and Article 14 on human oversight** of the AI Act apply to AI-native, zero-touch infrastructures.
- Promote **oversight-by-design approaches** as the primary means of complying with human oversight obligations in real-time 6G environments. Include architectural safeguards, predefined policy constraints, monitoring mechanisms and validated fallback modes, rather than real-time human intervention.
- Support **regulatory sandboxes and standardisation efforts** enabling telecom operators, regulators and standards bodies to test and validate compliant oversight architectures for AI-native network management before large-scale deployment.

Recommended policy



R4

Clarify accountability across complex 6G ecosystems

As 6G networks evolve into highly distributed, multi-vendor ecosystems, reinforcing governance structures becomes essential to maintain trust and legal clarity. Enhancing role assignments, contractual obligations, and oversight mechanisms would **strengthen accountability in data-rich multi-vendor 6G systems,** ensuring that each actor's responsibilities are clearly defined, consistent, and enforceable. Such measures also help **reduce disputes and improve breach handling,** enabling faster coordination, clearer escalation paths, and more effective remediation when incidents occur. By clarifying who is responsible for which processing operations, they **increase users' ability to identify the parties accountable for their data,** supporting meaningful rights exercise in complex infrastructures. At the same time, harmonised accountability models and transparent role delineation would **enable regulators to audit complex infrastructures effectively,** equipping supervisory authorities with the tools needed to assess compliance across interdependent supply chains. Together, these steps are crucial to securing a trustworthy and rights-preserving 6G ecosystem. Recommended policy options are the following:

- Develop **standard contractual frameworks or approved codes of conduct** for 6G data-processing chains. Define **sector-wide templates** for controller-processor responsibilities, breach notifications and data subject request handling.
- Publish **6G processing scenario catalogues** (via e.g., EDPB opinions). Identify **pre-approved models** clarifying role assignments in typical 6G contexts.
- Create a **GDPR Art. 42 certification scheme** for 6G service providers. Requires transparency on roles, vendor oversight, and cooperation mechanisms.

3. Policy Recommendations

R5 Reconcile conflicting privacy interests within the value chain

In a 6G landscape where commercial incentives, state security interests, and user rights increasingly collide, **coordinated governance** is essential to safeguard fundamental values. A balanced and coherent policy approach is needed to avoid privacy being systematically overshadowed by commercial or state interests, ensuring that economic or security objectives do not undermine individual autonomy or trust. Strengthening **harmonisation** across Member States on how national security exceptions are applied would reinforce **EU cohesion, reducing fragmentation** and ensuring that privacy protections remain consistent even in sensitive contexts. At the same time, clearer rules and oversight mechanisms can promote legitimate data uses while preventing exploitative or rights-eroding practices, enabling innovation without enabling misuse. By embedding these principles into the regulatory and operational framework for next-generation networks, policymakers can facilitate the socially acceptable deployment of 6G, ensuring that the technology evolves in ways that command public confidence and reflect European democratic values.

- **Harmonise EU rules** on public authority access to telecom data. Ensure consistent safeguards and minimisation principles.
- Use **trade and procurement policy** to mitigate conflicting foreign laws. Require vendors to disclose foreign government access obligations or to avoid suppliers subject to such laws.
- Create a permanent **multi-stakeholder 6G ethics and governance forum** coordinated for instance by the EC or ENISA that bring together telecoms, civil society, regulators, and law enforcement to shape guidelines (e.g., prohibiting social scoring or pervasive tracking).

R6 Modernise legal rules for location data

6G networks introduce Integrated Sensing and Communication (ISAC), so that 6G networks will natively combine communication with environmental sensing capabilities, enabling centimeter-level positioning accuracy and passive objective detection. This means networks can continuously monitor physical spaces and user movements with unprecedented precision, potentially enabling invasive profiling and ambient surveillance even of non-subscribers. The e-Privacy Directive governs location data, but it was drafted before such precision was possible. Current regulations do not adequately limit the collection, retention, or secondary use of fine-grained geolocation data.

- Strengthen **location-privacy rules** to reflect increased precision and potential intrusiveness. This should ensure that regulatory safeguards keep pace with the far more granular sensing capabilities expected in 6G.
- Provide **clear DPA guidance** specifying that any secondary use of 6G location data must meet strict legal requirements, including necessity, proportionality, and user consent. Such guidance would give operators and service providers unambiguous expectations and reduce inconsistent interpretations across jurisdictions.
- Limit **access to 6G location data,** requiring case-by-case judicial authorisation and independent oversight for real-time tracking. This would help prevent disproportionate surveillance practices and reinforce democratic accountability.

3. Policy Recommendations

R7 Enforce privacy, data protection and security literacy

A limited public understanding of how 5G and 6G systems process personal data creates a silent yet systemic ethical risk. The opacity of these infrastructures weakens informed consent and public trust as they increasingly permeate everyday life through IoT, AI, and edge computing. Developers also tend to conflate privacy, data protection, and security, reducing ethical and legal questions to technical fixes and enabling systems that may be secure but still infringe fundamental rights. No dedicated ethics framework exists for 5G/6G, while public communication remains fragmented and overly technical. As a result, citizens lack accessible information and meaningful avenues to participate in data governance and policy design. Recommended policy options are the following:

- Require 6G operators to activate all standardised **security features** under the European Electronic Communications Code (EECC); **prohibit use or sale of exploitative tools** except for authorised bodies.
- Ensure **democratic access** to information on 6G and promote critical thinking through digital and data-literacy initiatives.
- Foster **university-level education and training programmes** to give developers a clear, shared understanding of the distinct yet complementary roles of privacy, data protection, and security.
- Establish an **Ethics Framework for 6G** to guide responsible innovation, driven by values, and rights-based deployment.
- Adopt **KVIs** to assess the wider sustainability and societal impacts of 5G/6G technologies.
- Promote **accountability and trustworthiness** among all actors in the 5G/6G ecosystem.
- Improve **communication of 6G benefits and risks** to ensure informed public engagement.

R8 Reinforce targeted research and coordinated policy support

In conclusion, targeted research and coordinated policy support are needed to address the full set of challenges identified across the five priority risk areas. The next EU research framework should therefore include **dedicated CSA calls** designed to equip policymakers, regulators, data protection authorities, and standards bodies with the evidence, guidance, and operational frameworks required to act on these recommendations. These CSA should promote the following activities:

- Conduct **interdisciplinary legal and social-science deep research** on user control, algorithmic decision-making, profiling restrictions, cross-border transfers, sovereignty implications in 6G environments, and ultra-precise localization tracking.
- Identify **specific accountability gaps** caused by multi-vendor distributed infrastructures, opaque data flows, and automated network management.
- Deep **EU guidance for telecom-specific interpretations** of GDPR provisions (e.g., Article 22) and security standards, profiling limits, and responsibilities in shared data processing scenarios, defining **KVIs** to assess the wider sustainability and societal impacts of 6G technologies on privacy and data protection.
- **Produce policy blueprints** for sector-specific rules tailored to next-generation connectivity, supporting coherent regulation and enforceable responsibilities across the 6G value chain.
- Define **a code of conduct, an Ethics framework for 6G and a certification scheme** for 6G service providers as well as **training programs** for university-level education.
- Providing **clear, accessible information on 6G impacts** through public outreach, education, and transparent reporting.

4. Evidence and analysis

The project's findings are based on a triangulation of quantitative (surveys), qualitative (interviews and workshops), and desk-research methods, ensuring robustness and alignment between citizen, expert, and institutional viewpoints. Survey responses reflect the perceptions of participants rather than the full EU population, while evidence from SNS JU projects represents early-stage research rather than deployed infrastructures. Nevertheless, the extensive combination of scientific literature, citizen surveys, participatory workshops, interviews with industry practitioners and experts in acceptance, 6G, green ICT, smart cities and sustainability, as well as consultations with policy makers and engagement within the SNS JU community, provides complementary academic, civic, and institutional perspectives on how societal values are currently represented and operationalised in 6G research and innovation, and where alignment with EU frameworks such as the GDPR and the AI Act may require further action.

Across these activities, **privacy consistently emerged as the value most at risk** in the 6G context. Survey data indicate that 47% of citizens view privacy and data protection as their top concern for future connectivity, highlighting anxieties about **pervasive sensing, surveillance, and opaque uses of personal data.** Workshop participants echoed these concerns, emphasising the need for transparency, meaningful consent, and limits on AI-driven decision-making. SNS JU projects further substantiated these trends, with over 70% identifying privacy as a priority, particularly in relation to **sensing technologies, data ownership, and the use of network data for AI training.** Expert interviews confirmed a broader shift from traditional privacy concerns to deeper anxieties about **surveillance architectures, algorithmic control, and the erosion of digital autonomy.** These findings closely correspond to the **priority risks** outlined above.

5. Sources

This policy brief synthetises findings from 6G4Society Deliverables D1.1 [10], D1.2 [11] and D1.3 [12], as well as WP2 and WP3 outputs on stakeholder engagement and liaison with the SNS JU community. It draws on EU legal frameworks including GDPR, ePrivacy, Data Act, AI Act, Cyber Resilience Act, European Electronic Communications Code (EECC), as well as EU policies, strategies, guidelines and recommendations including Digital Decade 2030 (by DG CNECT), Cybersecurity of 5G networks (by EC), WP29 and EDPB guidelines and opinions, EU Toolbox for 5G Security and other ENISA reports.

Bibliography

[1] T. Zerdick, "“EDPS Blog – European Cybersecurity Month 2020: Time for clarity on 5G, security and privacy in the “new normal”," 19 October 2020. [Online]. Available: https://www.edps.europa.eu/press-publications/press-news/blog/european-cybersecurity-month.

[2] EDPB, "Guidelines 02/2024 on Article 48 GDPR," June 2025. [Online]. Available: https://www.edpb.europa.eu/system/files/2025-06/edpb_guidelines_202402_article48_v2_en.pdf.

[3] "Joint Statement Endorsing Principles for 6G: Secure, Open & Resilient by Design," 28 February 2024. [Online]. Available: https://2021-2025.state.gov/joint-statement-endorsing-principles-for-6g-secure-open-and-resilient-by-design/.

[4] WP29, "Guidelines on Automated Individual Decision-Making and Profiling for the purposes of Regulation 2016/679," 03 October 2017. [Online]. Available: https://ec.europa.eu/newsroom/article29/items/612053/en.

[5] ENISA, "ENISA 5G Threat Landscape," 14 December 2020. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

[6] ENISA, "ENISA 5G Security Controls Matrix," 24 May 2023. [Online]. Available: https://www.enisa.europa.eu/publications/5g-security-controls-matrix.

[7] C. Occhipinti, L. Briguglio, A. Carnevale, R. Santilli, E. Tangari, A. Iannone and Z. G. Pataki, "Privacy and Security aspects in 5G," CyberEthics Lab. & EPRS | European Parliamentary Research Service, March 2022. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/697205/EPRS_STU(2022)697205_EN.pdf.

[8] ENISA, "New Guidelines for Telecom and 5G Security," 10 December 2020. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/new-guidelines-for-telecom-and-5g-security?utm_source=chatgpt.com#contentList.

[9] ENISA, "EU Toolbox for 5G Security," January 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.

[10] 6G4Society, "D1.1: Societal aspects in 6G technology: concerns, acceptance models and sustainability indicators," 2024.

[11] 6G4Society, "D1.2 Towards a Socially Accepted and Sustainable 6G – Policy Brief.," 2025.

[12] 6G4Society, "D1.3 Towards a Socially Accepted and Sustainable 6G – Operational Brief.," 2025.

Contact

For further information, contact

https://cybersoclab.com/
eu-projects@cybersoclab.com

6G4Society Website
www.6g4society.eu

Project deliverables are publicly available through the **6G4Society Zenodo repository:**
https://zenodo.org/communities/6g4society

This work was supported by the 6G4SOCIETY project (Grant Agreement No. 101139070), which has received funding from the European Union's Horizon Europe research and innovation programme.

CyberSocialLab.