6G4SOCIETY

# TOWARDS A SOCIALLY ACCEPTED AND SUSTAINABLE 6G

*Dicember 2025*

## Operational Brief on Safeguarding Privacy in 6G

Carmela Occhipinti
Tetiana Vasylieva

CyberSocial Lab.

# 1. Highlights

The transition to sixth-generation (6G) mobile network marks a profound shift in the technological and societal landscape, one that goes far beyond a simple escalation in the amount of data being generated.

As highlighted in the 6G4Society policy analysis, 6G introduces **structural transformations in how data circulates, how responsibilities are distributed, how surveillance capabilities** intertwine with questions of digital autonomy and how user tracking, identification, and behavioural inference are impacted by 6G intrinsic capabilities.

Understanding these transformations as a network of interdependent dynamics is essential for translating 6G4Society policy recommendations into actionable guidance for industry. At the foundation of these transformations lie the 6G landscape characterised by **hyper-distributed architectures, AI-native functionality,** and **pervasive sensing capabilities.**

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 risks are not independent but mutually reinforcing: loss of user agency amplifies sensing-related intrusiveness; foreign access risks intensify accountability gaps; and opaque AI decisions compound existing asymmetries of power across the value chain.

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 operational 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:

- Integrate operational mechanisms strengthen user agency;
- Reinforce EU data sovereignty vs foreign access to EU data and supply-chain exposure;
- Embed accountability, oversight and transparency into AI-native network functions;
- Ensure accountability across multi-vendor 6G Ecosystems;
- Mitigate the societal risks of 6G Sensing and Positioning;
- Promote organisational and engineering literacy through unified technical guidelines.

# 2.Context of the Issue

The 6G environment will be characterised by continuous, often invisible streams of **environmental, behavioural, and positional data** produced by billions of devices. Such pervasive sensing challenges governance models that can't rely on explicit consent, user awareness, and clearly identifiable data controllers. In highly automated and ambient network environments, consent risks becoming episodic, symbolic, or detached from real data practices, requiring complementary operational safeguards beyond individual choice alone. In this context, restoring meaningful **user agency** becomes the first operational challenge: industries developing 6G technologies should design operational tools that are intended to allow individuals to understand and influence how their data is processed, even when the underlying systems are complex, dynamic, and automated. User control, however, cannot be considered separately from broader structural issues such as **privacy-by-design** and **data sovereignty.** The call for personal data spaces and interoperable tools requires industry stakeholders (such as for instance device manufacturers, cloud and edge providers, and network operators) to **embed granular consent management and transparent** data practices directly into their products and services.

At the same time, data sovereignty is not merely a political principle but a concrete operational constraint: making decisions such as for instance **routing choices, data-localisation strategies, and vendor selection** are all directly shaped by the need to protect European data from foreign ac-cess regimes and ensure legal certainty. Building user agency therefore depends on industry's ability to align technical infrastructures, governance models, and supply-chain decisions with European principles of autonomy and accountability. In operational terms, this implies that architectural decisions traditionally framed as purely technical (e.g., routing logic, orchestration layers, data replication strategies) become de facto privacy and rights-impacting choices that must be docu-mented, justified, and auditable. AI-driven net-work intelligence adds another layer of interdependence to the picture. As 6G networks rely increasingly on autonomous optimisation, behavioural analytics, and real-time decision-making, profiling and automated decisions become central to the functioning of the system. This creates direct implications for fairness, explainability, and individual rights. Industry should adopt **AI models that can be documented, audited, and scrutinised;** prevent **sensitive inferences** by design;

and ensure that **human oversight** remains possible for critical functions such as for instance resource allocation, intelligent handovers, and edge orchestration. In addition, **clear, enforceable accountability across the multivendor ecosystems** that characterise 6G infrastructure should be granted. This is strictly connected to the necessity of **supply-chain transparency, contractual clarity, and role definition.** As 6G distributes its processing chain across numerous actors handling different segments of the same data flow, there might be the high risk that **responsibility gaps** grow. Fragmented bilateral agreements are no longer sufficient; the industry requires **harmonised contractual frameworks, scenario-based mappings of processing roles, and certification schemes** that make **accountability** visible and verifiable, contributing to enhancing user control, AI governance and data sovereignty. emerging European AI governance requirements by embedding transparency, traceability, and human oversight directly into network functions rather than treating them as ex-post compliance obligations. These practices anticipate and operationalise Without such mechanisms, accountability risks remaining theoretical, undermining both regulatory compliance and public trust in complex multi-vendor environments.

All these measures are inseparable from the broader governance landscape: without **user agency,** sensing becomes uncontrollable; without **data sovereignty,** it becomes vulnerable to foreign exploitation; without **supply-chain accountability,** sensing becomes opaque.

The complexity of the value chain also creates deeper structural tensions. As highlighted in the policy analysis, **privacy, commercial interests, and national security do not simply coexist.** In some cases, they even collide. Operators wish to monetise data for analytics and new services; companies that deliver digital services over the internet depend on granular data for personalisation and targeted advertising [1]; governments demand access for security and law enforcement. The industry should be prepared to navigate these competing pressures by designing **privacy-respecting monetisation models,** implementing **independent audit** and **logging functions,** and building architectures capable of **supporting proportionate, accountable interventions by public authorities.**

Integrated Sensing and Communication (ISAC) exemplifies this interdependence. Unlike previous generations, 6G will incorporate **ultra-precise positioning and ambient sensing** into the very foundations of the network. These capabilities carry profound societal im-plications, enabling forms of continuous tracking, identification without interaction, and high-resolution behavioural inference [2]. Unlike previous generations, these inferences may occur without any explicit user action or service interaction, further challenging traditional notice-and-consent models.

Interface-based trans-parency mechanisms implicitly assume an active user engaging with a service and fail to protect the passive by-stander—individuals moving through sensed environments with no application, interface, or practical means to signal refusal. To address this gap, industry should support the development of protocol-level signalling mechanisms, through standardi-sation bodies such as 3GPP and ETSI, enabling **personal devices to broadcast a standardised "Do Not Sense" flag** that ISAC-enabled infra-structure would be required to recognise and enforce through automatic blinding or masking of sensing data. Industry should therefore adopt **adaptive sensing modes,** enforce **technical limits on granularity,** and select **partners capable of implementing data minimisation-by-design principles.** Underlying all of this is the need for **organisational literacy.** Meaningful progress depends on ensuring that everyone involved in designing, implementing, and deploying 6G systems shares a clear understanding of the **distinct roles and implications of privacy, data protection, and security.** Building a culture grounded in responsibility, minimisation, and transparency, and **equipping engineers and developers with interdisciplinary skills,** is essential. Equally crucial is promoting a cultural transformation, communicating clearly with citizens about how 6G technologies work, what data they process, and how individuals can exercise their rights. Finally, research, innovation, and standardisation should close the loop **adopting a value-driven architecture** to avoid bias, control intrusiveness, and ensure accountability.

Research and innovation should be guided by **codes of conduct and technical standards** that can be applied directly in real-world systems. In conclusion, user control, AI governance, data sovereignty, supply-chain accountability, sensing and geolocation safeguards, business-model design, organisational literacy, culture transformation, and value-oriented research should be understood as components of one integrated ecosystem. In this context, the 6G4Society Policy Brief provides the normative and strategic foundations; the Operational Brief translates them into **concrete industrial development practices** aiming at supporting the 6G sector to evolve in accordance with European values and individual's fundamental rights, trustworthy, resilient, and socially legitimate 6G infrastructure.

# 3.Operational Recommendations

## R1 Integrate operational mechanisms to strengthen user agency

The pervasive and often invisible data flows inherent to 6G networks risk leaving individuals without a clear understanding of who processes their data and how, making user agency increasingly difficult to exercise in practice. To ensure that 6G technologies uphold user autonomy, transparency and trust, industry actors must embed operational mechanisms that make data practices intelligible, manageable and enforceable. This includes enabling personal data spaces for telecom and sensing data, ensuring **clear identification of data controllers,** and providing straightforward ways for individuals to **exercise their data-protection rights.** These measures allow individuals to meaningfully control their 6G-related data and understand the functioning of pervasive sensing, AI-native optimisation and distributed network architectures.

- Establish an **EU-wide 6G Personal Data Space,** with standardised APIs allowing users to view, aggregate and modify permissions for all telecom-derived and sensing-related data.
- Introduce **mandatory digital and physical data-controller labels** for 6G and IoT devices, using a harmonised identifier that links directly to simplified rights-request and opt-out mechanisms.
- Require operators to **integrate clear user-facing information modules** into apps and portals, explaining what 6G data is collected and providing accessible controls for access, deletion, restriction of processing and other data-subject rights.
- Ensure that **usage and effectiveness** of these tools (e.g., access requests submitted, permissions modified, opt-outs exercised) are monitored as operational indicators of user agency.

## R2 Reinforce EU data sovereignty vs foreign access to EU data and supply-chain exposure

As 6G infrastructures rely on globally distributed supply chains and cross-border data flows, European data becomes increasingly exposed to foreign jurisdictions and interference risks, challenging the EU's ability to safeguard autonomy and legal protections. To uphold European data sovereignty in 6G, industry must implement technical and organisational measures that **ensure EU data remains protected from foreign access regimes, high-risk supply-chain dependencies, and uncontrolled cross-border flows.** This requires operational choices in routing, vendor selection, architecture design and data-handling methods that align day-to-day engineering practice with strategic autonomy and privacy protections.

- Adopt **sovereignty-aware routing and orchestration algorithms** that prioritise EU-based paths and edge resources by default, automatically avoiding data transit through third-country jurisdictions unless technically unavoidable.
- Integrate **vendor-risk scoring** into network design tools, ensuring that components from high-risk suppliers are excluded from data-rich or security-critical segments (e.g., sensing modules, AI orchestration layers, subscriber databases).
- Implement **local-processing and EU-only storage defaults,** using edge nodes, micro-data centres and trusted EU cloud services to ensure that raw sensing data, identifiers and inference-related metadata do not leave EU territory.
- Apply **strong encryption, key-splitting and hardware-root-of-trust mechanisms** so that, when cross-border transfers are unavoidable, foreign jurisdictions cannot access decipherable data or inference profiles.
- Create **auditable data-flow maps for all 6G services,** documenting where data travels, which vendors process it, and which jurisdictions are involved—allowing operators to demonstrate sovereignty compliance and rapidly remediate unwanted foreign exposure.

PRIVACY

## R3 Embed accountability, oversight and transparency into AI-native network functions

As 6G shifts towards autonomous optimisation, behavioural analytics and real-time AI-driven network decisions, the risk of unfair treatment, opaque inferences, and loss of human control increases. To enhance the **trustworthiness** of AI models, maintain system legitimacy and, at the same time, protect individual rights, industry must embed accountability, oversight and transparency directly into AI-native network functions. This requires models that can be documented and audited, mechanisms that prevent sensitive inferences, and operational safeguards ensuring that meaningful human intervention remains possible when network decisions have significant or irreversible effects.

1. Develop **auditable AI models and decision pipelines** by maintaining structured model documentation, versioning, input/output tracing, and explainability metadata for all optimisation, handover, orchestration and analytics functions. Couple these mechanisms with secure logging and retention policies enabling ex-post investigation of contested or harmful decisions by regulators or oversight bodies.

2. Implement inference-prevention modules that **automatically block or degrade the accuracy of AI models** when they risk producing sensitive behavioural inferences (e.g., health patterns, political tendencies, social relationships) from telecom data.

3. Adopt **privacy-preserving learning and distributed analytics techniques,** such as federated learning or edge-constrained training, to avoid centralising raw behavioural data while still enabling performant AI-native network intelligence, thereby reducing systemic risks while preserving the autonomy and responsiveness required by AI-native 6G networks.

4. Introduce **architectural human-oversight mechanisms** for high-impact operations—such as mobility prediction, edge orchestration or prioritisation decisions—through the use of deterministic safety monitors and sandboxing patterns. Rather than relying on real-time human intervention, which is infeasible in sub-millisecond 6G environments, AI components should be wrapped by **non-AI control layers that enforce pre-defined safety, policy and performance bounds defined by human operators** responsible for system design. When AI outputs fall outside these bounds, the system should automatically block the action and revert to a validated safe baseline. This approach operationalises the **human oversight requirement under Article 14 of the EU AI Act through oversight-by-design,** rather than active intervention, which represents the only viable implementation path for real-time 6G network functions.

## R4 Ensure accountability across multi-vendor 6G Ecosystems

Responsibility gaps in multi-vendor 6G environments undermine societal values such as accountability and justice. To ensure meaningful redress and clear traceability across complex supply chains, account-ability must be engineered directly into network architecture and operational workflows. Technology should make responsibility **transparent, auditable and enforceable** across all vendors, components and processing stages. Operational options are:

- Deploy **cryptographic provenance** systems that record which vendor processed which data, at which stage, and using which model or algorithmic component.
- Adopt **transparent chain-of-responsibility registries,** providing regulators and supervisory authorities with verifiable mappings of actors, roles and data-processing responsibilities.
- Synchronise **fault-tracking and incident-response** APIs across vendors, ensuring coordinated accountability, rapid remediation and consistent escalation procedures in multi-actor infrastructures.

## R5 Mitigate the societal risks of 6G Sensing and Positioning

The societal implications of ISAC (such as continuous tracking, object detection and behavioural inference) combined with the largely invisible nature of sensing, require that **transparency, proportionality and minimisation, purpose limitation and accountability** be engineered directly into 6G infrastructures. The ultra-precise positioning and ambient sensing capabilities of 6G significantly increase the intrusiveness and sensitivity of location data, making traditional safeguards insufficient. Operational options are:

1. **Transparency:** Provide **network-level transparency feeds** disclosing which sensing modes, inferences or automated actions are active in specific contexts. Equip **devices with local transparency agents** summarising the categories of data processed by nearby 6G nodes. Standardise **machine-readable transparency descriptors** allowing third-party apps to generate simple, citizen-oriented explanations of sensing activities.

2. **Proportionality and minimisation:** Introduce **adaptive sensing and precision-reduction mechanisms** that automatically lower spatial resolution when high accuracy is not technically required. **Apply minimisation-by-architecture,** ensuring raw, high-resolution environmental or location data is processed locally, with only abstracted or anonymised results shared across the network. Architect **edge-first processing pipelines,** keeping raw location and sensing data at the device or local edge node, with only aggregated or anonymised positioning information propagated to the wider network. **Support protocol-level opt-out mechanisms, such as a standardised "Do Not Sense" signal broadcast by personal devices,** requiring ISAC-enabled infrastructure to exclude the corresponding physical target from high-resolution sensing, storage and inference pipelines, except where strictly necessary for immediate system operation.

3. **Purpose limitation:** Implement **context-aware sensing policies,** reducing environmental scanning or positioning precision near sensitive locations or during low-risk operations. Tag **all location data streams with machine-readable purpose and retention metadata,** enabling automated enforcement of necessity, proportionality and consent requirements across services and vendors.

4. **Accountability and No Repudiation:** Deploy **tamper-evident access-logging systems** capturing requester identity, purpose, timestamp and authorisation for all fine-grained location queries. Use **strict role-based access controls (RBAC)** within network management and analytics platforms to ensure only authorised personnel or processes can access high-precision location information, and enabling **auditability of the enforcement of opt-out and minimisation signals** at infrastructure level.

PRIVACY

## R6

## Promote organisational and engineering literacy through unified technical guidelines

The complexity of 6G infrastructures—marked by pervasive sensing, AI-native optimisation and deeply distributed supply chains—requires a level of organisational literacy and multidisciplinary collaboration that goes beyond traditional telecom engineering. Without a shared understanding of how privacy, data protection and security should be interpreted and operationalised, inconsistencies emerge that undermine both user trust and regulatory compliance. To ensure that 6G technologies evolve in line with European values and fundamental rights, industry should **not only adopt common technical countermeasures** (e.g., Blockchain, Quantum Computing, explainable AI, Quantum Key Distribution, Post-Quantum Technology, etc.) **and Privacy Enhancing Technologies** (e.g., data anonymisation, pseudonymisation, zero-trust architectures, differential privacy, etc.). Although they are valid measures, they are not sufficient. Organisations should also cultivate interdisciplinary teams that integrate legal, ethical and engineering expertise, and embed Key Value Indicators (KVIs) into development processes so that societal impacts such as privacy, fairness and accountability are systematically measured and acted upon. Operational options are:

1. Draft SNS JU engineering **guidelines that define shared best practices** for secure, privacy-preserving, accountable and sovereignty-aware 6G design, implementation and deployment.

2. Integrate **KVI-based tools** into development and deployment pipelines, supporting organisations on identifying users desires and privacy-related societal values impacting the 6G technology especially in case of vertical use cases, enabling organisations to continuously track how design choices impact those societal values, and to adjust architectures proactively when risks increase.

3. Run structured **cross-disciplinary training modules,** bringing together telecom engineers, AI specialists, data-protection lawyers, ethicists and social scientists to ensure that technical teams understand and can operationalise legal, ethical and societal requirements in 6G architectures.

4. Establish **multidisciplinary design reviews** as a mandatory stage of the product development lifecycle, ensuring that privacy-by-design, minimisation, explainability, and accountability considerations are assessed jointly by technical, legal and ethical experts before deployment.

# 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 policymakers 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-native 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 operational brief synthesises findings from 6G4Society Deliverables D1.1 [3] and D1.2 [4], 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]** S. Zuboff, “The Age of Surveillance Capitalism,” Public Affairs, New York, 2019.
**[2]** H. Nissembaum, “Privacy in Context,” Stanford University Press, 2010.
**[3]** 6G4Society, “D1.1: Societal aspects in 6G technology: concerns, acceptance models and sustainability indicators,” 2024.
**[4]** 6G4Society, “D1.2 Towards a Socially Accepted and Sustainable 6G – Policy Brief.,” 2025.
**[5]** 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.