Centre for Information Policy Leadership
HUNTON

Designing for Safety: Addressing Real-World Risks in Data-Driven Environments

Key Recommendations and Practical Solutions

July 2026

Introduction

Over the past decade, digital technologies have transformed how we interact, work, and live. Many core services and activities in our daily lives are now conducted online, delivering significant benefits for individuals' daily lives as more time is spent online. At the same time, this can also introduce new risks; the online world can translate into offline harms such as theft, fraud, or danger to physical safety, resulting in a loss of trust in the online world. Some of these risks disproportionately affect specific groups of individuals, such as women, children, the elderly, or LGBTQ+ communities.

With malicious actors becoming increasingly adept at bypassing traditional safeguards, now also aided by AI, the timely detection of harmful behaviour has become significantly more difficult. In response, organisations across both the private and public sectors are turning to data-driven tools, including biometric and identity-based systems, to better manage these risks and maintain trust in key sectors and services.

Against this backdrop, the Centre for Information Policy Leadership (CIPL) convened a high-level roundtable with industry and regulatory leaders to examine how advanced technologies can mitigate risks and enhance trust and safety both online and offline and what potential barriers to broader adoption would have to be addressed.

The issues raised in the discussion are relevant to any jurisdiction in which data protection frameworks operate in tension with safety and security imperatives, whether imposed by law or expected by users. The roundtable focused on the GDPR, its UK equivalent and related European instruments such as the DSA and the OSA as key examples, but the underlying dynamic recurs across many legal systems while others, such as Brazil's LGPD with its express fraud-prevention ground, point in a more promising direction. The considerations and recommendations in this paper are therefore transferable in principle beyond the European frameworks discussed here.

This report reflects the considerations that emerged during the roundtable with regulators, policymakers and organisations regarding data processing for safety and security purposes. Key concerns that informed the discussion included:

- Regulators, policymakers and organisations should consider online and offline safety and security in a continuum and as a key imperative.

- In many safety and security contexts, biometric and identity-based tools can deliver more reliable verification than knowledge-based or document-only alternatives, provided they are deployed with appropriate accuracy testing, bias mitigation and proportionality safeguards.

- The current interpretation of EU data protection law, particularly the narrow reading of Article 9(2) exceptions and the limited availability of substantial-public-interest grounds for private-sector safety processing, creates legal uncertainty for organisations seeking to deploy proportionate biometric safeguards, often resulting in less effective alternatives being used by default.

Adapting to Change: Industry Approaches to Emerging Risks

Globally, organisations are continuously reassessing existing design choices in response to evolving threats and technological change, from static safety models to more dynamic, often biometric-enabled approaches.

Examples include:

Categories	Data-driven solutions
Safety and security	**Biometric video liveness checks** Converts facial data into numerical representations to prevent banned individuals from re-entering under new identities. **AI-driven behavioural analysis (audio/video)** Detects suspicious or threatening behaviour and enables remote human intervention when needed. **Real-time ID verification for service providers** Ensures that individuals offering in-person or physical services are authenticated before interaction. **Multi-factor identity validation** Combines a government-issued ID with a selfie image to strengthen identity verification. **AI-based risk detection** AI models analyse images and text (e.g., signs of self-harm or abuse) to flag potential risks for review.
Fraud prevention	**Advanced biometric ID verification** Includes liveness detection to prevent spoofing and deepfake-based attacks. **On-device biometric authentication for transactions** Flags irregular payments and requires biometric confirmation (e.g., fingerprint or face recognition). **Biometric payment cards** Cards with built-in fingerprint sensors that verify identity locally before completing transactions. **Voice recognition for phone banking** Authenticates users based on unique vocal patterns. **Palm recognition for cardless payments** Enables secure transactions without physical cards or devices.
Human verification	**Real-time age assurance and identity tools** Verifies age and identity before granting access to platforms or services. **Pre-access biometric verification** Confirms a user's identity at registration, before they can access a service or interact with others, as deployed on verified-only platforms. **Facial biometric verification via video selfie** Confirms: The person is real (liveness); The face matches the profile images; The same face is not used across multiple accounts. **Biometric identity checks in hiring** Confirms that a candidate is who they claim to be and connects them to their verified records, supporting large-scale remote recruitment where in-person checks are impractical. **Biometric room access** Uses facial or other biometrics to grant hotel room entry, reducing reliance on physical keys/cards.

The Current Landscape: The Same Safety Tools Are Not Available Across All Jurisdictions

While the available technologies are technically mature and already deployed at scale in many jurisdictions, the main barriers to their adoption are often legal and regulatory uncertainty, which may result in the implementation of more established knowledge- or document-based alternatives. Several recurring constraints emerged:

The legal basis for processing biometric and other special-category data. In the EU and UK, for instance, Article 9 GDPR (and its UK equivalent) sets out an exhaustive list of conditions for processing special-category data, which are of limited application in the online-offline safety context. Consent, for example, may not be available in the employment context due to the limiting assumption of a general balance of power between employer and employee; in fraud and abuse contexts, a consent requirement allows the bad actors to opt out of detection. The vital-interests exception attaches to the data subject and cannot readily be relied on to keep a bad actor off a platform. The substantial-public-interest ground requires a basis in Union or Member State law, which, for private-sector safety processing, largely does not yet exist.

Organisations are caught between safety mandates and data protection constraints. In the EU, while platforms may face safety obligations under the DSA or the OSA, those obligations do not themselves provide a legal basis for processing personal data under the GDPR. As the EDPB has noted, compliance with the DSA is not, in itself, a GDPR legal basis; there is currently no separate EU instrument, however, that expressly authorises the use of biometric or other identity-verification technologies solely to satisfy those obligations. Users have the expectation that the services they engage with will support the objectives of safety. Organisations are therefore expected to deliver safety outcomes while navigating questions with respect to implementing effective means of achieving them.

> Example: A manufacturer of driverless public-transport vehicles faces concerns that, without a driver present to potentially intervene, especially female passengers face a safety risk. However, it faces uncertainty as to the legal framework governing the deployment of audio- and video-based behavioural analysis tools that would enable a remote operator to detect threats and intervene when necessary.

Legal uncertainty remains a significant barrier to deploying safety-enhancing technologies in Europe. Organisations face divergent interpretations of data protection requirements across jurisdictions, particularly regarding the necessity and proportionality of processing, making it difficult to implement consistent solutions, especially across the EU. As a result, organisations may be reluctant to roll out safety tools that have demonstrated measurable benefits elsewhere, including in the context of age-assurance, identity-verification, and account-integrity features that help detect bad actors and reduce harmful interactions. The consequence is a potential protection gap, whereby some users may receive lower levels of safety protection than users in other regions despite the availability of effective safeguards.

> Example: A dating platform's video liveness check, a short selfie completed at registration and used to detect duplicate accounts, keep previously banned offenders off the service and support age assurance, was reported to have reduced users' exposure to bad-actor accounts by around 60% in the markets where it launched; it now covers a majority of the platform's users worldwide but has not been launched in Europe. Comparable in-app safety and identity-verification features offered by ride-hailing and delivery platforms are deployed across most of their markets, but not, or not fully, within the EU.

Recommendations for Safety-by-Design and Privacy-by-Design Digital Architecture

1. Apply Context-Driven, Risk-Based Interpretations of the GDPR Provisions (Article 6 and Article 9 GDPR)

Regulators should consider the widespread risks and harms prevalent across digital platforms when interpreting the application of legal bases under the GDPR and other data protection laws. Progressive interpretations that move beyond narrow applications, in particular of Article 9 GDPR, are necessary to empower organisations to adopt cutting-edge safety and security practices. Additionally, policymakers may need to address legal lacunae to enable data processing for safety and security reasons.

Context Matters: Regulators and policymakers should assess data processing for safety and security purposes in light of the specific risks organisations are seeking to address and the responsibilities they bear toward users, employees, products, and services. As online and offline threats become more sophisticated, the most effective safety measures will increasingly rely on the processing of personal data, and in some cases sensitive data, to detect, prevent, and respond to harm. Data protection rules should be interpreted and applied in a manner that enables responsible, risk-based processing for legitimate safety and security objectives, while maintaining appropriate safeguards and accountability. An overly restrictive approach can create unintended barriers to the deployment of proven protection measures.

- **Article 6 GDPR:** Promote the application of contract, legitimate interest, vital interest, public interest and legal duty as appropriate bases for processing data for safety and security reasons.
- **Article 9 GDPR:** Where appropriate, processing biometric data for safety and security purposes may be grounded in substantial public interest (Article 9(2)(g)) or, in narrowly defined emergency contexts, the vital interests exception (Article 9(2)(c)). Reliance on Article 9(2)(g) requires a basis in Union or Member State law providing for suitable and specific measures; Member States and the Commission should clarify and, where necessary, legislate substantial public interest grounds for specified safety purposes, such as fraud prevention, age assurance, and the protection of users from documented online-to-offline harms.

Limitations of Consent: Consent is not always the most appropriate legal basis for safety and security processing. In certain contexts, for example, employment, consent may not meet the GDPR's "freely given" standard; in fraud-prevention contexts, requiring consent can undermine the underlying purpose of the processing, for instance, by signalling protective measures to bad actors, or by allowing the individual most likely to be engaged in fraudulent activity to opt out of detection. Both the GDPR (and the EDPB in their guidance) recognise that legitimate interest, not consent, is the principal basis for fraud-prevention and network-security processing.

Digital Omnibus Proposal: The Commission's Digital Omnibus proposal would introduce a new Article 9(2)(l), permitting the processing of biometric data where necessary to confirm a data subject's identity, provided the biometric data or the means needed for verification remain under the data subject's sole control. This is a welcome recognition that the risk of biometric processing depends on the modality of use, one-to-one verification rather than one-to-many identification, and not on the data category alone. The sole-control condition, however, confines the ground to on-device verification and would not reach the platform-side safety measures described in this paper. The underlying problem remains the classification of biometric data as sensitive per se, combined with an exhaustive list of legal bases; a contextual, use-based approach would offer a more proportionate and future-proof foundation for safety and security processing.

UK Data Use and Access Act (Data Act) 2025: The UK Data Act 2025 introduces the concept of a "recognised legitimate interest" as a new legal basis for processing data. In Annex 1, the Data Act establishes that the detection and prevention of a crime, such as fraud, and the protection of an individual at risk, among other purposes, are recognised legitimate interests. In some cases, organisations can rely on recognised legitimate interests to process data without needing to complete a Legitimate Interests Assessment (LIA). This basis operates within Article 6 UK GDPR, however, and does not in itself authorise the processing of special-category data such as biometrics; a separate Article 9 assessment remains necessary.

2. Evolve beyond Legal Bases and Towards Enhanced Accountability

Building trustworthy and safe digital platforms is not simply a question of identifying a legal basis for processing. Rather, it requires a holistic approach to responsible data governance. While establishing a lawful basis for safety and security-related processing is an essential first step, organisations must also ensure that such processing is transparent, proportionate, accurate, secure, and subject to appropriate oversight and safeguards, such as the implementation of privacy-enhancing technologies. Compliance, therefore, extends beyond Articles 6 and 9 GDPR to encompass the full range of GDPR obligations, including accountability, purpose limitation, data minimisation, and the protection of individuals' rights. In this way, organisations can deploy effective safety measures while maintaining trust and demonstrating responsible stewardship of personal data.

3. Align and Integrate Regulatory Compliance

To avoid fragmented compliance, both regulators and organisations must consider safety, security and data protection holistically, through an aligned and integrated lens.

Integrated Risk Assessments: Regulators should support governance frameworks that enable organisations to assess privacy, safety, security, fraud, and abuse risks in an integrated and proportionate manner. Decisions about the deployment of biometric or identity-based safety measures should be informed by a holistic evaluation of the risks, benefits, and safeguards associated with the processing, including the potential impact on users, third parties, and other fundamental rights and interests. Moving away from siloed compliance exercises toward integrated risk assessments would promote more effective accountability, improve risk management, and help organisations balance privacy protections with legitimate safety and security objectives.

> ⓘ Example — Retention and Security Must Be Considered Together: Data retention decisions should be assessed in light of both data protection principles and organisations' safety and security responsibilities. While storage limitation and data minimisation remain important safeguards, retention periods that are determined solely through a narrow privacy lens may undermine an organisation's ability to detect fraud, identify repeat offenders, investigate harmful conduct, and protect users over time. For example, effective account-integrity measures often cannot rely exclusively on a one-time verification at registration. Instead, they may require the ongoing assessment of behavioural indicators and patterns over time, which in turn necessitates retaining certain data for longer periods. Regulators should therefore recognise that appropriately calibrated retention periods can be an essential component of responsible safety and security programmes and should be evaluated in the context of the risks being mitigated and the safeguards applied.

Treat Privacy, Safety, and Security as Complementary Objectives: Privacy, safety, and security are all grounded in fundamental rights and should not be viewed as inherently competing interests. In practice, effective protection of individuals often requires balancing these objectives and recognising their interdependence. Data processing undertaken to prevent fraud, detect abuse, protect vulnerable users, or enhance security can play an important role in safeguarding individuals' rights and freedoms. Regulatory frameworks should therefore encourage holistic assessments that consider the impact of both action and inaction, enabling organisations to deploy proportionate and accountable measures that advance privacy, safety, and security together rather than treating them as mutually exclusive goals.

Recognise the Risks of Inaction: Risk assessments should take into account not only the risks arising from data processing, but also the risks associated with failing to process data where such processing is necessary to protect individuals and services. Fraud, repeated abuse by previously banned users, unauthorised access to age-restricted services, grooming, harassment, and other forms of harm can have significant consequences for individuals and communities. These risks often fall disproportionately on vulnerable populations and may undermine the very rights and interests that data protection frameworks seek to safeguard. Regulators should therefore support a balanced and context-specific approach to proportionality assessments that considers both the risks of processing and the risks of inaction when evaluating legitimate interests, substantial public interest grounds, and AI governance obligations.

4. Promote Proactive, Collaborative and Risk-Based Regulatory Behaviours

As digital technologies become increasingly central to economic and social life, regulatory approaches should support the responsible use of data to advance privacy, safety, security, and innovation. Regulators and policymakers should encourage governance models that provide organisations with the clarity, confidence, and accountability needed to develop and deploy effective solutions to emerging digital risks.

Promote Early and Ongoing Engagement

Regulators and organisations should engage proactively throughout the design and development lifecycle of products and services involving novel or higher-risk processing. Early dialogue can help identify and address risks, improve compliance outcomes, and enable the deployment of solutions that deliver meaningful benefits to individuals and society.

Expand Regulatory Sandboxes and Innovation Programmes

Governments and regulators should promote the use of regulatory sandboxes, innovation testbeds, and other structured mechanisms that allow organisations to test and refine new technologies in controlled environments. Such programmes should provide meaningful regulatory certainty and incentives for participation, enabling organisations to innovate responsibly without fear that engagement itself will create additional regulatory exposure.

Adopt Risk-Based Oversight

Regulatory guidance, supervisory activities, investigations, and enforcement actions should be proportionate to the actual risks and benefits associated with the processing. A risk-based approach allows regulators to focus resources on activities that present the greatest potential for harm while supporting responsible innovation and effective risk mitigation.

Strengthen Cross-Regulatory Coordination

As oversight of digital platforms increasingly spans privacy, consumer protection, competition, online safety, cybersecurity, and AI governance, regulators should work together to ensure coherent and consistent regulatory outcomes. Greater coordination can reduce legal uncertainty, avoid conflicting obligations, and support more effective compliance. Initiatives such as the UK Digital Regulation Cooperation Forum demonstrate the value of structured collaboration across regulatory authorities. Policymakers should strengthen and expand such mechanisms, including through formal cooperation frameworks, information-sharing arrangements, and coordinated guidance where appropriate, to promote greater consistency, efficiency, and regulatory certainty across the digital ecosystem.

5. Develop and Promote Technical Standards that Embed Trust by Design

Technical standards can play an important role in translating complex legal requirements into practical, scalable, and interoperable solutions. Well-designed standards can help organisations advance safety, security, privacy, and accountability objectives simultaneously, while providing greater certainty for innovation and implementation.

Adopt a Holistic "By Design" Approach

Organisations should integrate Privacy-by-Design, Security-by-Design, Safety-by-Design, and Accountability-by-Design principles throughout the product and service lifecycle. These objectives are mutually reinforcing and should be considered together rather than in isolation.

Support Standards for Biometric Technologies

Public-private collaboration can help develop robust technical, governance, and assurance standards for biometric technologies and related data processing. Common standards can improve trust, interoperability, transparency, and accountability while enabling organisations to deploy biometric solutions responsibly and consistently across jurisdictions.

6. Strengthen Transparency and Explainability

Transparency and explainability are foundational to trust in the digital ecosystem. As organisations increasingly deploy advanced technologies to enhance safety and security—including solutions that may involve sensitive data such as biometric information—they should ensure that individuals understand how and why such processing occurs, the safeguards that apply, and the benefits the processing is intended to deliver. Transparency should evolve beyond compliance-focused notices toward more meaningful, accessible, and user-centred communication.

Communicate Purpose and Value

Organisations should clearly explain the purpose, rationale, and expected benefits of data processing, particularly where novel technologies or techniques are used to improve safety, security, or user protection.

Demonstrate Accountability in Practice

Transparency should extend beyond describing processing activities to explaining the safeguards, governance measures, security controls, and limitations on secondary uses that protect individuals and build trust.

Prioritise Meaningful Transparency

Organisations should focus not only on meeting the formal requirements of transparency obligations but also on ensuring that information is understandable, relevant, and actionable for the intended audience.

Encourage Participatory Approaches

Regulators and organisations should explore collaborative approaches to transparency and explainability, including user testing, stakeholder engagement, and co-design initiatives. Experiences such as the UK ICO's regulatory sandbox programmes demonstrate the value of involving affected users directly in the development and evaluation of transparency measures.

7. Strengthen Transparency and Explainability

Transparency and explainability are foundational to trust in the digital ecosystem. As organisations increasingly deploy advanced technologies to enhance safety and security—including solutions that may involve sensitive data such as biometric information—they should ensure that individuals understand how and why such processing occurs, the safeguards that apply, and the benefits the processing is intended to deliver. Transparency should evolve beyond compliance-focused notices toward more meaningful, accessible, and user-centred communication.

Communicate Purpose and Value

Organisations should clearly explain the purpose, rationale, and expected benefits of data processing, particularly where novel technologies or techniques are used to improve safety, security, or user protection.

Demonstrate Accountability in Practice

Transparency should extend beyond describing processing activities to explaining the safeguards, governance measures, security controls, and limitations on secondary uses that protect individuals and build trust.

Prioritise Meaningful Transparency

Organisations should focus not only on meeting the formal requirements of transparency obligations but also on ensuring that information is understandable, relevant, and actionable for the intended audience.

Encourage Participatory Approaches

Regulators and organisations should explore collaborative approaches to transparency and explainability, including user testing, stakeholder engagement, and co-design initiatives. Experiences such as the UK ICO's regulatory sandbox programmes demonstrate the value of involving affected users directly in the development and evaluation of transparency measures.

8. Continuously Reassess Risks and Adapt Safeguards

Safety, security, privacy, and fraud risks are dynamic and continuously evolving. Technologies, threat actors, user behaviours, and societal expectations change over time, and governance frameworks must evolve accordingly. Effective risk management, therefore, requires ongoing monitoring, reassessment, and adaptation rather than one-time compliance exercises.

Design for Continuous Improvement

Organisations should periodically reassess risks, safeguards, and mitigation measures throughout the lifecycle of a product or service and adjust their approaches as technologies, threats, and user expectations evolve.

Anticipate Emerging Risks and Opportunities

Product design decisions that are appropriate at one point in time may become ineffective as bad actors develop new techniques or as new technologies create opportunities for enhanced protection. Organisations should maintain processes that enable them to identify emerging risks and responsibly deploy improved safeguards where appropriate.

Support Adaptive Governance

Regulatory frameworks should recognise that responsible innovation often requires iterative testing, learning, and refinement. Encouraging ongoing evaluation and adaptation can help organisations maintain effective protections while continuing to meet privacy, security, and accountability obligations.

Summary of Recommendations

The recommendations developed in this paper are summarised below. Taken together, they describe an integrated approach to safety, security and data protection enabling proportionate, trustworthy data processing for safety and security purposes.

Apply context-driven, risk-based interpretations of GDPR legal bases

Recognise contract, legitimate interest, vital interest, public interest and legal duty as appropriate Article 6 grounds for safety processing; use Article 9(2)(g) for biometric processing where Member State law provides suitable safeguards; acknowledge the structural limits of consent in safety and fraud-prevention contexts; build on the Digital Omnibus's proposed biometric-verification ground (Article 9(2)(l)) towards a contextual, use-based treatment of biometric data.

Evolve beyond legal bases towards enhanced accountability

Scale accountability to the sensitivity of the use case; apply strict purpose limitation and proportionate data minimisation rather than categorical bans; deploy PETs such as tokenisation, encryption, secure enclaves and federated learning.

Align and integrate regulatory compliance

Conduct integrated risk assessments covering data protection, security, fraud and abuse; weigh the risk of inaction alongside processing risks in Article 6(1)(f), Article 9(2)(g) and AI Act assessments.

Promote proactive, collaborative and risk-based regulatory behaviours

Engage ex-ante on high-risk projects; expand sandboxes with the right incentives; calibrate guidance and enforcement to actual risks; strengthen cross-regulatory cooperation (e.g. UK DRCF, EDPB Cooperation Subgroup).

Develop technical standards with "by Design" principles

Integrate Safety-, Accountability-, Security- and Privacy-by-Design; advance biometric standards through public-private partnerships modelled on the ICO-Yoti sandbox.

Improve transparency and explainability

Move beyond formal notices to meaningful, accessible disclosure; honour the "spirit" of Articles 12-15 GDPR; co-create explainability tools with users, including children where relevant.

Revisit product design decisions

Treat safety, security and privacy assessments as continuous; reassess as threats, technologies and user behaviours evolve.

Extend liability across the entire stack

Allocate accountability and incentives across the full safety stack, including specialised third-party vendors, so responsibility follows actual control.

1 For example, through the currently ongoing Digital Omnibus process.

2 EDPB, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (October 2024), para 29.