Centre for Information Policy Leadership
HUNTON

CIPL's Big Ideas

for Simplification of Europe's Digital Rulebook

November 2025

Contents

Foreword

Europe has led the world in placing people at the centre of the digital economy. The GDPR built global trust in data use, and the EU has since created the most comprehensive digital rulebook of any major jurisdiction. It has driven higher standards worldwide and strengthened Europe's voice in global debates.

As the digital rulebook has expanded, so too has its operational complexity. Rules created at different moments and for different purposes increasingly intersect. Organisations now navigate parallel requirements for risk assessment and incident reporting, while individuals face repeated notices and consent fatigue. This complexity is not the price of strong protection; at times, it obscures it.

Europe does not need a new model. It needs to refine and streamline the one it has, building digital trust while ensuring implementation is risk-based, coherent and workable at scale. This paper sets out twenty-seven big ideas for reform that maintain high standards, reduce friction and focus effort on real-world outcomes. They fall into five themes:

- **Making smart, surgical updates to Europe's data laws** – refreshing core rules on sensitive data, purpose limitation and automated decision-making to enable responsible innovation with strong safeguards
- **Removing friction and resolving contradictions across the digital rulebook** – aligning privacy and safety duties, joining up digital competition and data protection laws, and harmonising data mobility rules
- **Creating and incentivising a coherent, trusted system of digital accountability** – establishing common governance expectations so organisations can design once and demonstrate compliance consistently
- **Equipping regulators with modern, agile tools and practices** – embedding sandboxes, impact assessment, risk-based enforcement and structured cooperation across regulators
- **Building regulatory readiness for change** – encouraging regulators to use existing powers and flexibilities to unlock innovation, target serious harms and act consistently and impactfully

Taken together, these measures maintain Europe's leadership in rights and trust, strengthen enforcement against genuinely harmful practices and deliver simpler, more effective compliance for responsible organisations. They support innovation and competitiveness without compromising the values at the heart of European digital policy.

This is not a choice between ambition and protection. Europe can and should do both. By updating key rules, aligning regimes and modernising regulatory practice, Europe can safeguard fundamental rights while enabling secure, trustworthy and competitive digital services for the decade ahead.

Bojana Bellamy
President, Centre for Information Policy Leadership

Part 1: Make smart, surgical updates to Europe's data protection laws

Europe has long been at the forefront of global data protection efforts. But after almost a decade of rapid technological change, some rules need fine-tuning to maintain trust, reduce friction and support responsible innovation. Targeted modernisation can reinforce rights while enabling beneficial uses of data in health, security, research and everyday services.

Here, we set out seven targeted updates to GDPR and ePrivacy rules – from scrapping blanket cookie consent requirements to updating automated decision-making rules for the age of AI. Together, these reforms will:

- give **people** fairer, better and more straightforward digital experiences;
- enable **organisations** to use data and AI responsibly under practical, workable rules;
- equip **regulators** with firmer mandates and a sharper focus on genuinely high-risk practices; and
- anchor **Europe** in a rights-preserving model that strengthens global competitiveness and public trust.

Big Idea #1: Modernise purpose limitation to enable responsible data reuse

Why change is needed

The GDPR requires organisations to limit data use to specific purposes, defined at the point of data collection. Yet in a world of AI and continually evolving digital services, many socially valuable future uses, such as improving fraud detection, cybersecurity or model safety, cannot always be precisely defined at the point of collection. This can push organisations towards seeking consent for reuse even where people cannot meaningfully understand or control how their data will be used, or where consent is simply impractical at scale. The result is unnecessary friction for responsible data use and slower progress on beneficial innovation, even where strong safeguards are in place.

What change is needed

Purpose limitation prevents people's data from being reused in ways they would not reasonably expect. This protection is essential when data is processed with consent, where people's choices and expectations anchor the legitimacy of the processing. But other lawful bases – legal obligation, public task, vital interests, contract and legitimate interests – do not rely on what was said at the point of collection in the same way. Their legitimacy comes from statutory duties, emergencies or a balancing test, not from consent to a specific purpose.

Europe should therefore evolve purpose limitation so that it applies only where it protects individual agency. Where data were collected with consent, organisations must seek fresh consent if the new purpose is incompatible. But where data were collected under other lawful bases, organisations should be able to reuse them for new purposes provided the new purpose is grounded in a valid lawful basis – for example, a new legitimate-interests assessment, a new legal obligation or an activity within a public authority's mandate –

supported by clear transparency, necessity and safeguards.

This would create a more coherent, basis-driven system: strict purpose control where autonomy depends on it, and pragmatic, accountable reuse elsewhere. It would reduce friction, support safe and socially valuable innovation and maintain strong protection for individuals' expectations and rights.

Big Idea #2: Reimagine rules for sensitive data to unlock fair, responsible AI and data use

Why change is needed

The GDPR treats data such as health, biometrics or ethnicity as highly sensitive in all circumstances. In today's environment, that can block valuable and low-risk uses – from training medical models and improving health apps to checking AI systems for bias. Organisations are often pushed towards seeking consent, even when this offers little real choice or is impractical at scale. At the same time, genuinely risky practices can escape scrutiny simply because they do not fall neatly into existing legal categories.

What change is needed

Europe should adopt a modern, risk-based approach to sensitive data that focuses on how the data is used, rather than assuming all sensitive categories present the same risk. Under this model, organisations could rely on lawful routes beyond consent where they can show that:

- using sensitive data serves a legitimate organisational or societal interest (e.g. bias mitigation);
- no less intrusive alternative exists to achieving the goals of the data use; and
- the benefits of the data use clearly outweigh the impact on people.

In making this judgement, organisations would need to assess what individuals would reasonably expect, how sensitive the data are in context and the strength of the safeguards in place. The bar for data use would remain higher than for less sensitive data.

This would improve fairness, accuracy and quality of services for the public, support innovation in areas such as health and safety and give responsible organisations a workable route to use data well and reinforce Europe's reputation for trusted, values-driven technology.

Read more: Rethinking Sensitive Data in the Age of AI (CIPL, 2025)

Big Idea #3: Update automated decision-making rules for the age of AI

Why change is needed

Automation can deliver faster, more consistent and more accurate outcomes in services ranging from fraud detection and credit decisions to healthcare triage and digital public services. Yet current rules treat solely automated decisions with significant effects as prohibited unless narrow conditions are met, with regulators taking an increasingly expansive view of what decisions fall in scope. This discourages responsible deployment, drives risk-averse compliance and limits innovation even where technology can improve fairness, accuracy and accessibility for individuals.

What change is needed

Europe should remove its default prohibition on solely automated decisions and instead introduce a clear set of rights that apply whenever a decision with significant effects is made without meaningful human involvement. Under this model, individuals would have:

- a right to a meaningful explanation of the decision and the factors that shaped it;
- a right to contest the decision; and
- a right to human review carried out by someone with the authority and competence to change the outcome.

Taken together, these rights would enable people to benefit from faster, better decisions with clear rights and meaningful recourse. They would also give responsible organisations clearer conditions for deploying trustworthy AI, while upholding protections.

Big Idea #4: Broaden research provisions to support public-interest innovation

Why change is needed

The GDPR allows personal data to be used for scientific research, with Recital 159 confirming that this should be interpreted in a "broad manner" – including privately-funded research and development. Yet in practice, these provisions are often interpreted as applying only to academic bodies or the public sector. This narrow reading creates uncertainty for commercial public-interest research and development, such as improving early detection of infectious disease, enhancing anti-fraud systems, developing safer medical devices and evaluating whether AI models perform fairly across different groups.

What change is needed

Legislators should clarify GDPR's research rules to ensure that they apply wherever activity is genuinely directed at public benefit, regardless of organisational form. This should be coupled with clear safeguards, including transparency, strong governance controls and, where feasible, pseudonymisation and privacy-enhancing technologies (PETs). Such clarification would provide a stable and predictable basis for responsible commercial research, enabling progress in areas such as health, safety and fraud prevention while maintaining high standards of protection.

Big Idea #5: Create a non-exhaustive list of recognised legitimate interests to support responsible data use

Why change is needed

The GDPR allows data to be used where an organisation has a legitimate interest, provided this is balanced against people's rights. In practice, however, uncertainty about what qualifies means organisations default to seeking consent for beneficial processing, even where people cannot meaningfully choose or control use. This creates unnecessary bureaucracy for individuals and adds cost and complexity for organisations trying to innovate.

What change is needed

Europe should set out in law a non-exhaustive list of recognised legitimate interests. These should include

tackling fraud, preventing cyber attacks, responsibly training and testing AI models, ensuring products and services remain safe, improving essential services and supporting public-interest research and evaluation. Organisations would still need to show that processing is necessary and proportionate, use only the data required and protect it effectively. This would reduce consent fatigue, support responsible operational uses of data and improve regulatory consistency across Member States.

Read more: How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation (CIPL, 2021)

Big Idea #6: Remove blanket cookie-consent rules and rely on the GDPR instead

Why change is needed

Currently, the ePrivacy Directive requires consent before placing cookies and similar technologies even when used simply to keep a service secure, functioning and reliable, with only narrow exemptions for uses that are strictly necessary to provide a service. These blanket prompts were intended to protect privacy, but most people click through without engaging, while intrusive tracking still occurs elsewhere.

What change is needed

Lawmakers should repeal Article 5(3) of the ePrivacy Directive and rely on the GDPR alone to govern cookies and similar technologies. Low-risk uses, including security, service functionality, fault resolution, performance measurement and contextual advertising, could rely on legitimate interests or another appropriate basis, provided people are given clear information and the ability to object. Intrusive profiling that cannot meet the legitimate interests test would still require consent. This shift would simplify browsing experiences for people, reduce consent fatigue and direct consumer and regulatory attention towards genuinely high-risk tracking practices.

Big Idea #7: Enable recognition of trusted international data frameworks, including CBPR, where they meet EU standards

Why change is needed

Europe has set the global benchmark for data protection. Yet international transfers remain complex and resource-intensive even where strong protections exist. Organisations often repeat similar transfer assessments and contractual measures, creating cost without improving outcomes. Many jurisdictions now operate GDPR-inspired privacy regimes, and trusted frameworks such as the Global Cross-Border Privacy Rules (CBPR) system have introduced independent oversight, enforceable rights and government access safeguards.

However, EU law currently provides only two formal routes: adequacy for entire jurisdictions (which can be slow and complex) and contractual or organisational mechanisms for individual transfers. There is no clear pathway to recognise more agile, credible international systems that meet EU standards for essential equivalence and redress. This creates unnecessary friction for routine cross-border operations, even where individuals face very low risk and oversight is strong.

What change is needed

The EU should introduce a complementary legal route that allows recognition of independent privacy frameworks, such as CBPR, where they demonstrably deliver protections equivalent in substance to EU law. Recognition should:

- apply to certified organisations, not entire jurisdictions;
- require proven safeguards, rights and redress, including limits on government access;
- involve regular review, with rapid suspension powers where standards fall; and
- sit alongside, not replace, adequacy and existing transfer mechanisms.

This would create a tightly-controlled pathway for trusted entities that can evidence real-world safeguards. It would preserve strong protection for people while enabling more efficient, predictable transfer arrangements for responsible organisations. It would also support a more coherent global ecosystem in which EU-level safeguards travel with the data, regardless of jurisdiction.

Read more: Global CBPR and Global PRP Systems Playbook (CIPL, 2025)

Part 2: Remove friction and contradictions across the digital rulebook

Multiple EU digital laws now govern privacy, safety, competition, online content, cybersecurity, interoperability and access to data. While each regime serves an important public purpose, overlaps and misalignments can create confusion, conflict and inefficiency for people, regulators and organisations. Clear alignment will protect rights more effectively, strengthen action to tackle genuine risks, and avoid unnecessary burden or delay.

In this section, we propose six reforms to align privacy and safety duties, streamline data mobility rules, reconcile competition and data protection requirements and improve coordination between regimes. Taken together, these changes will:

- give **people** clearer protections and simpler, more consistent experiences across digital services;
- help responsible **organisations** avoid duplication and conflicting obligations while strengthening real safeguards;
- enable **regulators** to act more coherently on cross-cutting issues and focus resources where they matter most; and
- support **Europe** in delivering a more integrated, innovation-ready Single Market rooted in strong values.

Big Idea #8: Align privacy and safety duties with clear, proportionate rules

Why change is needed

Europe's digital rules protect both privacy and safety. However, where these duties interact, uncertainty often arises. For example, where age assurance is required under the Digital Services Act (DSA), it can sit uneasily alongside GDPR data minimisation principles. Under the ePrivacy Directive, safeguards designed for commercial tracking can constrain proportionate child protection, malware detection and account integrity measures. In practice, organisations risk defaulting to blanket avoidance of protective tools or over-collection of data – with neither outcome serving individuals well.

What change is needed

Legislators should provide clear legal routes to process data to protect people from serious harm. The ePrivacy regime should introduce a narrowly defined legal basis for essential safety measures – for example to protect children, detect malware and prevent account compromise. Processing under this basis should remain highly targeted, strictly necessary and subject to strong safeguards to avoid general monitoring or unnecessary intrusion.

In parallel, age assurance and essential security logging could be recognised as legitimate interests (see Big Idea #5) under the GDPR, either in law or through guidance. This would be subject to a full balancing test and documented safeguards. Where such measures inevitably involve sensitive information, the GDPR's restrictions should be clarified and, where necessary, tailored to ensure proportionate safety measures remain lawful without weakening protections. This approach preserves

rights, maintains proportionality and strengthens public trust while enabling effective harm prevention.

Big Idea #9: Align DMA and GDPR rules on consent to improve the user experience and tackle consent fatigue

Why change is needed

The Digital Markets Act (DMA) prevents the largest platforms from combining data across their services without consent. The aim is to prevent practices that could entrench market power or limit consumer choice. In practice, however, the rule applies even where combining data is not likely to affect competition at all. Uses such as detecting fraud, securing accounts, improving product reliability or enabling basic cross-service functionality fall squarely into this category.

Under the GDPR, these same activities would normally be carried out under legitimate interest, supported by risk assessments, safeguards and governance controls. By forcing a consent prompt in these circumstances, the DMA does not strengthen competition; it simply adds friction, fuels "click-through" fatigue and distracts from genuine risks.

What change is needed

Legislators should make a targeted amendment to the DMA so that data needed for essential safety, security and service quality can rely on the GDPR's legitimate interest framework, provided the processing has no material impact on competition or user choice. This would align the DMA with established GDPR practice and remove unnecessary prompts for routine, low-risk operations. The DMA's existing restrictions on data uses that may affect competition would remain unchanged. This would reduce unnecessary friction for people and responsible organisations, while enabling regulators to focus on genuinely relevant data uses.

Read more: Limiting Legal Basis for Data Processing under the DMA (2023)

Big Idea #10: Align EU data mobility rules to support innovation, interoperability and trusted data sharing

Why change is needed

Europe now has multiple frameworks enabling data mobility: the GDPR (data portability), the DMA (continuous data access obligations for gatekeepers) and the Data Act (interoperability for connected products and cloud services). In parallel, the Data Governance Act establishes trusted intermediaries for secure data sharing.

Each regime pursues legitimate public goals. But they operate through distinct triggers, formats and permission models. For organisations building secure data-sharing interfaces, this can create overlapping engineering work, uncertainty over compliance routes and fragmentation in user consent and authorisation flows. The result is avoidable cost and slower progress on privacy-preserving interoperability.

What change is needed

The EU should establish a common permission and revocation model that all three frameworks recognise for user-initiated exports and continuous feeds, supported by standard security controls and audit. Definitions and data categories should be

mapped so like-for-like data are handled consistently, and technical interface standards should be harmonised where possible.

Such a unified model would help users understand and manage permissions more easily and create a more consistent experience across services. It would also streamline compliance for organisations building secure, user-centred interoperability tools. This approach preserves the purpose of each law while reducing friction and reinforcing Europe's model of secure, user-centred data access.

Read more: Data Sharing Obligations Under the DMA: Challenges and Opportunities (2024)

Big Idea #11: Bring relevant ePrivacy rules under the European Data Protection Board for consistent, efficient enforcement

Why change is needed

The GDPR introduced coordinated enforcement across Europe through the European Data Protection Board (EDPB). In contrast, ePrivacy rules remain enforced entirely at national level. Key privacy-facing elements – notably cookies, tracking and direct marketing – are interpreted and enforced differently across Member States, with divergent tests for consent, exemptions and interface design. Individuals experience different standards depending on where they live, and organisations face avoidable complexity and uncertainty. Fragmented enforcement wastes regulatory and industry resources without delivering better protection.

What change is needed

Legislators should bring oversight of relevant ePrivacy rules within the EDPB framework for cross-border matters. National authorities would continue to manage domestic matters and telecoms-specific issues, but where services or practices affect more than one Member State, regulators would cooperate through the same mechanisms used for GDPR enforcement. This would mean common guidance, consistent decision-making and joined-up investigations. Such alignment would reduce duplication, improve speed and ensure that protections are applied consistently across the Single Market. It would also give organisations a clearer supervisory pathway for cross-border issues.

Big Idea #12: Deliver digital fairness through existing laws, not new legislation

Why change is needed

Fairness, transparency and consumer protection are vital to a trusted digital economy. These objectives are already embedded across the GDPR, DSA, DMA, AI Act, Data Act and Unfair Commercial Practices Directive, which together regulate both business conduct and data use. Creating an additional horizontal law, such as a Digital Fairness Act, would risk overlap, inconsistency and uncertainty at a time when simplification and coherence are urgently needed.

What change is needed

The Commission should re-evaluate the need for a separate Digital Fairness Act and focus instead on coherent implementation of existing legislation.

CIPL's Big Ideas for Simplification of Europe's Digital Rulebook

Part 1: Make smart, surgical updates to Europe's data protection laws

Modernise purpose limitation to enable responsible data reuse

Reimagine rules for sensitive data to unlock fair, responsible AI and data use

Update automated decision-making rules for the age of AI

Broaden research provisions to support public-interest innovation

Create a non-exhaustive list of recognised legitimate interests to support responsible data use

Remove blanket cookie-consent rules and rely on the GDPR instead

Enable recognition of trusted international data frameworks, including CBPR, where they meet EU standards

Part 2: Remove friction and contradictions across the digital rulebook

Align privacy and safety duties with clear, proportionate rules

Align DMA and GDPR rules on consent to improve the user experience and tackle consent fatigue

Align EU data mobility rules to support innovation, interoperability and trusted data sharing

Bring relevant ePrivacy rules under the European Data Protection Board for consistent, efficient enforcement

Deliver digital fairness through existing laws, not new legislation

Part 3: Create a coherent, trusted system of digital accountability

Establish a common accountability framework across Europe's digital laws

Align GDPR and AI Act risk assessment requirements in law

Align user-facing transparency requirements across digital laws

Create a unified incident-reporting framework across digital laws

Part 4: Equip regulators with modern, agile tools and practices

Make regulatory sandboxes a legal requirement to accelerate responsible digital innovation

Require digital regulators to consider innovation, competition and growth when interpreting the law

Enable digital regulators to prioritise high-risk harms through risk-based supervision and enforcement

Establish consistent consultation standards for digital regulators to support transparent and effective rule-making

Require cooperation, consultation and information sharing across digital regulators

Part 5: Build regulatory readiness for change

Use the margin of manoeuvre within GDPR to enable practical, responsible innovation

Accelerate adoption of GDPR codes of conduct, certification schemes and binding corporate rules

Embed risk-based and outcomes-focused approaches across compliance, supervision and enforcement

Establish and expand regulatory sandboxes across Europe

Advance transparent and evidence-based regulatory decision-making

Consolidate and extend coordination across Europe's digital regulators

This should include developing practical guidance clarifying how existing laws already require fairness and transparency and promoting consistent, joined-up supervision and enforcement across regimes. Any further legislation should be limited to narrowly targeted updates where genuine legal gaps are demonstrated. This approach advances the same objectives while improving clarity and enabling regulators to focus on real-world outcomes rather than new legislation.

Part 3: Create a coherent, trusted system of digital accountability

Strong governance is the foundation of safe, fair and trustworthy digital services. Yet accountability duties have grown piecemeal across Europe's digital laws, often requiring organisations to create parallel structures to address similar risks. This fragments oversight, creates unnecessary cost and dilutes attention from the issues that matter most. A shared accountability baseline would strengthen protection, reduce duplication and create a clearer, more predictable system for both organisations and regulators.

In this section, we set out four reforms to align accountability expectations, harmonise risk assessments, streamline transparency duties and simplify incident reporting. Taken together, these measures will:

- give **people** clearer, more consistent safeguards across digital systems and services;
- allow **organisations** to build once and comply across regimes, reducing duplication and strengthening real accountability;
- equip **regulators** with comparable evidence and more coherent oversight tools; and
- support **Europe** in developing a more streamlined and innovation-ready Single Market grounded in trusted governance.

Big Idea #13: Establish a common accountability framework across Europe's digital laws

Why change is needed

Europe's digital rules rightly expect organisations to demonstrate strong internal governance. Yet governance duties have developed independently across the GDPR, AI Act, DSA, DMA and NIS2. This promotes separate oversight structures, parallel documentation and repeated assurance processes, even where the underlying risks overlap. The result is duplicated effort, fragmented decision-making and governance structures shaped by regulatory silos rather than real-world harms.

What change is needed

Legislators should move towards a harmonised accountability baseline across digital regimes, grounded in widely accepted principles. This foundation should cover:

1. **Leadership and oversight** – clear senior responsibility for compliance and risk
2. **Risk assessment** – structured evaluation of the risks and benefits to individuals, society and the economy and appropriate safeguards (see Big Idea #14)
3. **Policies and procedures** – proportionate, documented controls aligned to risk
4. **Transparency** – clear information for the public and regulators on rights and safeguards (see Big Idea #15)
5. **Training and awareness** – proportionate capability-building across relevant teams

6. **Monitoring and verification** – internal and, where appropriate, independent assurance
7. **Response and enforcement** – prompt remediation, learning and cooperation with authorities (see Big Idea #16)

This core framework should meet shared requirements across regimes, with additional obligations applied only where they are genuinely necessary to address distinct risks. This ensures consistency without creating a one-size-fits-all model, preserving the flexibility needed to reflect different risk environments while focusing effort where it matters most. The shared baseline would create clearer expectations and help organisations design systems that satisfy multiple regimes at once. It would also support more consistent supervisory practice across the EU.

Read more: What Good and Effective Data Privacy Accountability Looks Like (2020); Building Accountable AI Programs (2024)

Big Idea #14: Align GDPR and AI Act risk assessment requirements in law

Why change is needed

Under the GDPR and the AI Act, organisations deploying many AI systems will be required to conduct two separate assessments: a Data Protection Impact Assessment and a Fundamental Rights Impact Assessment. Both are designed to identify risks to individuals and ensure effective mitigation. If applied in parallel without alignment, these duties will lead to duplicated work, parallel documentation and unnecessary delay, without improving outcomes for people.

What change is needed

Legislators should harmonise the GDPR and AI Act risk assessment requirements so that a single assessment can satisfy both frameworks where it addresses the relevant risks, with additional modules only where genuinely distinct obligations exist. Core concepts – including assessing risks to individuals and defining appropriate safeguards – should be aligned in law to ensure coherence. This would maintain strong protections and focus effort on meaningful risk analysis rather than duplicative work.

Big Idea #15: Align user-facing transparency requirements across digital laws

Why change is needed

When people use digital services, several laws require organisations to explain how systems work and how data is used. The GDPR requires clear information on data use and rights before processing commences. The AI Act will require notice when AI systems are used and explanation of their key characteristics. The DSA introduces transparency duties for recommender systems and online ads. These obligations serve a common purpose but have developed separately, leading to overlapping requirements with differing wording, scope, format and timing. Without alignment, people risk receiving multiple, repetitive notices that are hard to navigate, while organisations face avoidable duplication.

What change is needed

Legislators should align key transparency obligations across the GDPR, AI Act and DSA so that one user-facing notice can satisfy shared requirements, with

modular additions only where specific regimes demand extra detail. Alignment should include when information must be provided, what must be explained, how rights are signposted and expectations on clarity and accessibility. Distinct disclosures should remain for genuinely unique risks, but the default should be coherence and clarity. This would give people more consistent and trustworthy information across services, streamline compliance for organisations, and support regulators with clearer, more comparable disclosures.

Big Idea #16: Create a unified incident-reporting framework across digital laws

Why change is needed

Europe's digital laws impose multiple duties to report incidents affecting security, data protection and online safety. The GDPR requires personal-data breaches to be notified within 72 hours. NIS2 requires significant cyber incidents to be reported within 24 hours. The Cyber Resilience Act, Digital Operational Resilience Act, ePrivacy Directive, Second Payment Services Directive (PSD2) and Digital Services Act all impose further reporting requirements. The same incident – such as a cyber intrusion – can trigger several overlapping reports and, in some cases, multiple notices to users or the public. This duplication can slow crisis response and does not improve protection.

What change is needed

Legislators should align incident-reporting thresholds, timelines and core content across Europe's digital laws, allowing organisations to make one primary notification with modular additions only where distinct risks justify extra information. The same principle should apply to user or public notification: one clear notice that meets shared requirements, with supplementary detail only where necessary. A common reporting gateway should support coordinated supervisory follow-up. This improves regulatory visibility while reducing unnecessary burden in moments that demand focus and speed.

Part 4: Equip regulators with modern, agile tools and practices

Effective regulation depends on strong capability, clear guardrails and evidence-based decision-making. As technology evolves, regulators must be able to test approaches early, prioritise the highest-risk harms and develop guidance in an open and transparent way. Modern tools and joined-up working will ensure high standards, public trust and a dynamic digital economy.

In this section, we set out reforms to make regulatory sandboxes routine, strengthen consultation and impact assessment practices, embed risk-based supervision and improve cooperation across authorities. Together, these measures will:

- give **people** clearer, faster and more reliable protection from serious digital harms;
- help **organisations** engage earlier with regulators and build compliant, trustworthy systems from the outset;
- improve **regulators'** technical capability, operational consistency and use of real-world evidence;
- position **Europe** as a leader in innovation-friendly, outcome-focused regulation that delivers results.

Big Idea #17: Make regulatory sandboxes a legal requirement to accelerate responsible digital innovation

Why change is needed

Europe's digital rules set high standards, but organisations often struggle to apply them to new technologies without clear, early guidance. Regulatory sandboxes offer a practical solution by allowing real-world testing under supervisory oversight. Yet outside the AI Act, availability of sandboxes depends on the discretion and resources of individual regulators.

What change is needed

Europe should extend the AI Act model and mandate regulatory sandboxes across key digital regimes, including GDPR and the Digital Services Act. This would provide lawful, structured routes to test and refine new approaches, enabling innovators to achieve compliance by design and regulators to build technical insight, strengthen guidance and evolve rules through practical evidence rather than theory. For the public, this means faster access to innovative services with safeguards built in from the outset.

Read more: Designing Effective Regulatory Sandboxes: Learning from Practice (CIPL, 2025)

Big Idea #18: Require digital regulators to consider innovation, competition and growth when interpreting the law

Why change is needed

Europe's digital laws give regulators significant discretion in how they interpret and apply them. These policy decisions can shape innovation, investment, competition and access to digital services. Without an explicit requirement to consider the public interest in responsible data use for innovation, competition and economic growth, well-intentioned regulatory choices can become overly cautious and slow beneficial technologies and services.

What change is needed

Legislators should introduce a duty for digital regulators to consider the impact of discretionary decisions on innovation, competition and economic growth, alongside duties to uphold rights and ensure legal compliance. For major interventions, such as new policy guidance, regulators should publish a concise impact assessment of likely costs, benefits and alternatives. This would encourage more balanced, evidence-led decisions that support responsible innovation and better outcomes for people.

Big Idea #19: Enable digital regulators to prioritise high-risk harms through risk-based supervision and enforcement

Why change is needed

Europe's digital regulators increasingly face complex harms, rapid technological change and finite resources. While many already seek to prioritise, statutory frameworks do not always give them the flexibility to focus consistently on the most serious and likely harms. This can hinder rapid responses to emerging risks and sustained action on high-impact issues.

What change is needed

Legislators should make clear that, where Union law affords discretion in supervision and enforcement, regulators may prioritise actions according to risk and significance of harm. Supervisory and enforcement decisions, including case selection and resource allocation, should be proportionate to risk and directed at securing effective, real-world protection. This would strengthen regulatory impact by ensuring that limited resources are directed to the areas where they deliver the greatest public benefit.

Read more: Getting the Best Outcomes: Pathways for Data Protection and Privacy Authorities (CIPL, 2024)

Big Idea #20: Establish consistent consultation standards for digital regulators to support transparent and effective rule-making

Why change is needed

Digital regulators increasingly shape how laws operate through guidance, opinions and other regulatory instruments. These decisions can have significant effects on compliance expectations, costs, innovation and the availability of digital services.

However, consultation practices vary across regimes, and in some cases guidance is introduced with limited external engagement. This can lead to uncertainty, inconsistent interpretation and avoidable burdens. Clear minimum standards for consultation would help ensure regulatory decisions are informed by practical experience, tested for real-world impact and supported by broad public confidence.

What change is needed

Legislators should introduce a consistent requirement for digital regulators to consult publicly before issuing major guidance, opinions or similar instruments that shape compliance expectations or impose material burdens. Consultations should be proportionate to impact, include meaningful engagement with affected groups, and provide transparency on evidence considered and alternatives assessed. Where regulators prepare an impact assessment this should also be subject to consultation, so that regulators are able to receive wider evidence on costs and benefits. This approach would ensure that regulatory expectations are clear, workable and grounded in the public interest.

Big Idea #21: Require cooperation, consultation and information sharing across digital regulators

Why change is needed

Europe's digital landscape is now governed by multiple regulatory bodies, spanning data protection, AI, online safety, competition, cybersecurity, interoperability and consumer protection. Many organisations therefore face oversight from several regulators at once, sometimes with overlapping or even conflicting expectations. While cooperation mechanisms exist in some regimes, they are uneven and coordination can vary in practice. This risks fragmented guidance, duplicated compliance demands and slower intervention in cases of harm. Clear, consistent cooperation duties would help regulators align approaches, reduce burden and deliver better protection for people, markets and society.

What change is needed

Legislators should introduce cooperation duties across digital regulatory frameworks to ensure join-up between competent authorities. Regulators should be required to consult one another when issuing guidance or decisions that have significant horizontal impact, to ensure alignment and avoid regulatory conflicts. In addition, lawmakers should establish proportionate legal gateways to enable timely information sharing between regulators where this is necessary to protect individuals or ensure coherent supervision.

Combined with a duty on innovation, competition and economic growth (see Big Idea #18), these measures should ensure that regulators take a holistic view rather than operating in silos. Cooperation and information sharing should remain practical and proportionate, allowing regulators to act swiftly where required while promoting clarity and consistency across the digital regulatory environment.

Part 5: Build regulatory readiness for change

Simplification will only succeed if regulators model it first. Without waiting for new legislation, regulators can use existing powers and flexibilities to unlock innovation, target serious harms and act consistently and impactfully. Investing in this culture change will lay the foundations for a more effective and competitive European framework.

In this section, we set out actions that regulators can take now – from pragmatic interpretation of GDPR principles to enhanced regulatory cooperation and clearer strategic prioritisation in supervision and enforcement. Together, these actions will:

- ensure **people** benefit sooner from safer, more trusted and more innovative digital services;
- enable **organisations** to develop, test and deploy innovative services with greater confidence, supported by clear expectations and strong safeguards;
- strengthen **regulators'** capability, confidence and alignment across jurisdictions;
- put **Europe** on a stronger footing to introduce a modernised digital framework that upholds rights and supports competitiveness.

Big Idea #22: Use the margin of manoeuvre within GDPR to enable practical, responsible innovation

Why change is needed

The GDPR provides regulators with discretion to interpret core principles such as fairness, purpose limitation, data minimisation and transparency in context. Yet this flexibility is often under-used, leading to rigid compliance expectations that discourage responsible experimentation and slow socially valuable innovation. Consistent, transparent interpretation can uphold rights while allowing proportionate, evidence-based approaches to develop.

What change is needed

Data protection authorities should use their lawful discretion within the GDPR and existing Court of Justice of the European Union (CJEU) case law to clarify how core principles apply in practice.

Working collectively through the EDPB, regulators should publish coordinated examples and guidance illustrating balanced approaches – for instance, providing illustrative lists of legitimate interests recognised under existing law or refreshing practical anonymisation standards building on the CJEU's Single Resolution Board (SRB) ruling. Guidance should be transparent, consistent across Member States and clearly reasoned, showing how flexibility strengthens protection by focusing oversight on areas of genuine risk while enabling innovation consistent with the law's intent and without weakening individual rights.

Big Idea #23: Accelerate adoption of GDPR codes of conduct, certification schemes and binding corporate rules

Why change is needed

The GDPR created powerful mechanisms to translate principles into practice through approved codes of conduct, certification schemes and binding corporate rules. Yet uptake remains limited. Complex approval processes and inconsistent expectations between authorities have slowed progress, leaving a major opportunity untapped. Widespread adoption would turn these mechanisms into practical tools for demonstrating accountability, raising sectoral standards and ensuring consistent protection across borders.

What change is needed

Data protection authorities, supported by the EDPB, should streamline and accelerate the approval of codes, certification schemes and binding corporate rules (BCRs). This includes publishing model criteria, templates and evaluation checklists to ensure predictable and efficient review, and pooling expertise across Member States to share workload. Approved schemes should incorporate independent oversight, transparency obligations and demonstrable improvements over baseline compliance. Adherence should carry meaningful weight in supervision and enforcement decisions, rewarding organisations that invest in verified, rights-preserving accountability frameworks.

Read more: The GDPR's First Six Years: Positive Impacts, Remaining Implementation Challenges, and Recommendations for Improvement (CIPL, 2024)

Big Idea #24: Embed risk-based and outcomes-focused approaches across compliance, supervision and enforcement

Why change is needed

Digital regulators face complex, fast-changing technological risks and finite resources. Process-driven oversight can diffuse effort and encourage formalistic compliance rather than genuine accountability. A structured, risk-based and outcomes-focused approach enables regulators to target serious or systemic harms, concentrate resources where they matter most and deliver measurable protection for people while supporting responsible innovation.

What change is needed

Digital regulators should make full use of the discretion afforded in legislation to prioritise supervision and enforcement according to the severity and likelihood of harm. Each authority should set out statements of their strategic priorities and adopt proportionate assurance and monitoring for lower-risk activity, such as complaint handling. Enforcement should focus on securing tangible improvements for individuals and society, with transparent reasoning and public reporting on how decisions reflect risk and expected outcomes. Across Europe, this approach should enhance rather than reduce enforcement by directing effort to the most serious, likely or systemic infringements, ensuring high standards of protection for all individuals.

Big Idea #25: Establish and expand regulatory sandboxes across Europe

Why change is needed

Regulatory sandboxes enable responsible testing of new technologies under supervisory oversight. As proposed in Big Idea #17, future legislation should make them a formal duty. In the meantime, many regulators already have sufficient powers to operate voluntary sandboxes but few do so. Consolidating existing efforts will help regulators build capability, share insights and prepare for a harmonised model once required in law.

What change is needed

Digital regulators should expand or launch sandboxes within current mandates, operating under full compliance and clear participant safeguards. Participation should not alter legal obligations and must remain subject to supervisory control throughout. Where possible, regulators should seek to join these initiatives up across sectors and borders, ensuring that regulators provide joined-up advice. Pan-European institutions including the EDPB and European AI Office should coordinate a network linking these initiatives, sharing learning and best practice. Findings should feed into guidance that strengthens protection standards and prepares for the wider sandbox framework envisaged in Big Idea #17.

Read more: Designing Effective Regulatory Sandboxes: Learning from Practice (CIPL, 2025)

Big Idea #26: Advance transparent and evidence-based regulatory decision-making

Why change is needed

Digital regulators already exercise wide discretion when interpreting complex and fast-moving laws. As highlighted in Big Ideas #18 and #20, these choices shape both fundamental rights and economic growth. Yet consultation and impact assessment practices are uneven, which makes it harder for regulators, industry and civil society to build shared understanding. Strengthening transparency, listening and dialogue now will support trust and smoother implementation ahead of any future law reform.

What change is needed

Digital regulators should consult publicly and proportionately on major guidance, opinions and policy initiatives, engage early with a wide range of stakeholders and be clear about the questions on which they seek evidence. They should publish a short impact assessment covering effects on fundamental rights and economic growth, and explain how feedback informed the final outcome. Networks such as the EDPB should promote best practice in consultation, engagement and impact assessment to encourage consistency across regimes.

Big Idea #27: Consolidate and extend coordination across Europe's digital regulators

Why change is needed

As set out in Part 2, Europe's digital laws increasingly overlap across privacy, safety, competition, cybersecurity and AI. Digital regulators are increasingly cooperating through joint consultations (for example the EDPB and the European Commission's joint consultation on DMA–GDPR guidelines), but approaches still differ in scope and impact. Consolidating and extending this collaboration would improve coherence, consistency and clarity.

What change is needed

Digital regulators should build on existing partnerships by coordinating guidance on shared issues, aligning public messaging where appropriate and exchanging lessons from cross-regime supervision. Successful national models, such as Ireland's Digital Regulators Group – which brings together the Data Protection Commission, Coimisiún na Meán, ComReg and the Competition and Consumer Protection Commission – provide an example that other Member States can emulate. Extending similar collaboration at EU level will help deliver more consistent protection for people and clearer expectations for industry across Europe.