Contribution ID: c4277cc2-f439-4f87-afea-abb332225009
Date: 11/03/2026 20:20:58

Public Consultation on the Digital Fitness Check

Fields marked with * are mandatory.

Introduction

The Commission is committed to deliver tangible results in support of the EU's competitiveness, not least through an ambitious simplification agenda, as outlined in the Communication on 'A Simpler and Faster Europe ', translating the political vision of President von der Leyen's Political Guidelines into a robust action plan for the implementation and the simplification of the rules.

Digital rules have been instrumental in framing a fair business environment in the EU. They established a true single market for digital services. Europe has pioneered digital regulation, and has set the gold standard for the highest level of protections for fundamental rights, consumer safety and the protection of our values. At the same time, the Draghi and Letta reports highlight that the accumulation of rules has sometimes had an adverse effect on competitiveness. Fast and visible improvements are needed for people and businesses, through a more cost-effective and innovation-friendly implementation of our rules – all the while maintaining high standards and core objectives of the rules.

The Commission took a first step to simplify the digital rulebook with the proposals of the Digital Omnibus. The Digital Fitness Check comes as a second step to stress-test the complementarity, efficiency and effectiveness of the rulebook. The fitness check is an evidence-based assessment of the cumulative impact, effectiveness, efficiency and EU added value of a series of rules. The Digital Fitness Check has a very wide scope, and this consultation is a first step through which the Commission seeks to focus the forthcoming analysis on the areas most pressing for the reality on the ground, and areas where there is a potential for further optimising the rules.

The Digital Fitness Check will focus on how the digital rulebook is affecting the competitiveness of businesses in the EU, in particular SMEs, focusing on areas of strategic importance for the Union, ranging from different technology development areas to media and creative industries. It will assess how different laws work together in practice – identifying synergies, as well as remaining gaps and inconsistencies. This, with a view to 'stress test' the application of the rules, amplify good practices and identify areas where further adjustments are needed.

This is part of a continuous effort to ensure that the digital rulebook remains effective, proportionate and fit for the future, and delivers on the EU's high standard of protection of fundamental rights.

You are invited to reply to this questionnaire and/or submit a paper. The Commission seeks your views on your direct experience with the application of EU digital rules. Your feedback will inform the Commission's scoping and in-depth analysis of the coherence and cumulative impact of the digital rules.

The Commission seeks to consult broadly, inviting all citizens, stakeholders and experts to respond to the consultation.

About you

* Language of my contribution

- ○ Bulgarian
- ○ Croatian
- ○ Czech
- ○ Danish
- ○ Dutch
- ◉ English
- ○ Estonian
- ○ Finnish
- ○ French
- ○ German
- ○ Greek
- ○ Hungarian
- ○ Irish
- ○ Italian
- ○ Latvian
- ○ Lithuanian
- ○ Maltese
- ○ Polish
- ○ Portuguese
- ○ Romanian
- ○ Slovak
- ○ Slovenian
- ○ Spanish

- ○ Swedish

* I am giving my contribution as
  - ○ Academic/research institution
  - ◉ Business association
  - ○ Company/business
  - ○ Consumer organisation
  - ○ EU citizen
  - ○ Environmental organisation
  - ○ Non-EU citizen
  - ○ Non-governmental organisation (NGO)
  - ○ Public authority
  - ○ Trade union
  - ○ Other

* First name

Charles

* Surname

LOW

* Email (this won't be published)

clow@accis.eu

* Organisation name

255 character(s) maximum

ACCIS - Data for credit

* Organisation size
  - ◉ Micro (1 to 9 employees)
  - ○ Small (10 to 49 employees)
  - ○ Medium (50 to 249 employees)

- ○ Large (250 or more)

Transparency register number

Check if your organisation is on the transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.

21868711871-63

* Country of origin

Please add your country of origin, or that of your organisation.

This list does not represent the official position of the European institutions with regard to the legal status or policy of the entities mentioned. It is a harmonisation of often divergent lists and practices.

- ○ Afghanistan
- ○ Åland Islands
- ○ Albania
- ○ Algeria
- ○ American Samoa
- ○ Andorra
- ○ Angola
- ○ Anguilla
- ○ Antarctica
- ○ Antigua and Barbuda
- ○ Argentina
- ○ Armenia
- ○ Aruba
- ○ Australia
- ○ Austria
- ○ Azerbaijan
- ○ Bahamas
- ○ Djibouti
- ○ Dominica
- ○ Dominican Republic
- ○ Ecuador
- ○ Egypt
- ○ El Salvador
- ○ Equatorial Guinea
- ○ Eritrea
- ○ Estonia
- ○ Eswatini
- ○ Ethiopia
- ○ Falkland Islands
- ○ Faroe Islands
- ○ Fiji
- ○ Finland
- ○ France
- ○ French Guiana
- ○ Libya
- ○ Liechtenstein
- ○ Lithuania
- ○ Luxembourg
- ○ Macau
- ○ Madagascar
- ○ Malawi
- ○ Malaysia
- ○ Maldives
- ○ Mali
- ○ Malta
- ○ Marshall Islands
- ○ Martinique
- ○ Mauritania
- ○ Mauritius
- ○ Mayotte
- ○ Mexico
- ○ Saint Martin
- ○ Saint Pierre and Miquelon
- ○ Saint Vincent and the Grenadines
- ○ Samoa
- ○ San Marino
- ○ São Tomé and Príncipe
- ○ Saudi Arabia
- ○ Senegal
- ○ Serbia
- ○ Seychelles
- ○ Sierra Leone
- ○ Singapore
- ○ Sint Maarten
- ○ Slovakia
- ○ Slovenia
- ○ Solomon Islands
- ○ Somalia

- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivia
- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Burkina Faso
- Burundi
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Greenland
- Grenada
- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Hong Kong
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar/Burma
- Namibia
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- Norfolk Island
- Northern Mariana Islands
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname
- Svalbard and Jan Mayen
- Sweden
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia
- Timor-Leste
- Togo
- Tokelau
- Tonga

- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d’Ivoire
- Croatia
- Cuba
- Curaçao
- Cyprus
- Czechia
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Russia
- Rwanda
- Saint Barthélemy
- Saint Helena Ascension and Tristan da Cunha
- Trinidad and Tobago
- Tunisia
- Türkiye
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
- Wallis and Futuna
- Western Sahara
- Yemen
- Zambia

- Democratic Republic of the Congo
- Lesotho
- Saint Kitts and Nevis
- Zimbabwe
- Denmark
- Liberia
- Saint Lucia

The Commission will publish all contributions to this public consultation. You can choose whether you would prefer to have your details published or to remain anonymous when your contribution is published. **For the purpose of transparency, the type of respondent (for example, 'business association, 'consumer association', 'EU citizen') country of origin, organisation name and size, and its transparency register number, are always published. Your e-mail address will never be published.** Opt in to select the privacy option that best suits you. Privacy options default based on the type of respondent selected

* Contribution publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

- **Anonymous**
  Only organisation details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.
- **Public**
  Organisation details and respondent details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published. Your name will also be published.

☑ I agree with the personal data protection provisions

1. Introductory questions

In which of these sectors are you or is your organisation active?

- ☐ Healthcare Mobility

- [ ] Transport and automotive
- [ ] Robotics
- [ ] Manufacturing and construction
- [ ] Climate and environment
- [ ] Energy
- [ ] Agrifood
- [ ] Defence, security and space
- [ ] Electronic communications
- [ ] E-commerce
- [ ] Media
- [ ] Cultural and creative sector
- [ ] Public services
- [x] Other

How many people does your organisation employ?

- [x] micro (1 to 9 employees)
- [ ] small (10 to 49 employees)
- [ ] medium (50 to 249 employees)
- [ ] small mid-cap (250-749 employees)
- [ ] large (750 or more employees)

Is your organisation headquartered in the EU?

- [x] Yes
- [ ] No

Is your parent company headquartered in the EU?

- [ ] Yes
- [ ] No

In which Member State(s) is your business active, i.e. where does it provide services or sell goods?

- ( ) AT - Austria
- (•) BE - Belgium

- ○ BG - Bulgaria
- ○ HR - Croatia
- ○ CY - Cyprus
- ○ CZ - Czechia
- ○ DK - Denmark
- ○ EE - Estonia
- ○ FI - Finland
- ○ FR - France
- ○ DE - Germany
- ○ EL - Greece
- ○ HU - Hungary
- ○ IE - Ireland
- ○ IT - Italy
- ○ LV - Latvia
- ○ LT - Lithuania
- ○ LU - Luxembourg
- ○ MT - Malta
- ○ NL - Netherlands
- ○ PL - Poland
- ○ PT - Portugal
- ○ RO - Romania
- ○ SK - Slovak Republic
- ○ SI - Slovenia
- ○ ES - Spain
- ○ SE - Sweden

If your organisation is active outside the EU, please specify below.

Do you give the European Commission's services permission to contact you for follow-up discussions or events related to the topics covered in your submission?

- ☑ Yes

- [ ] No

2. Opportunities supported by the Digital Rulebook

Digital rules have been instrumental in framing a fair business environment in the EU. They established a true single market for digital services instead of a fragmented business environment across Member States, promoting the competitiveness of businesses across the EU. Europe has pioneered digital regulation, and has set the gold standard for the highest level of protections for fundamental rights, consumer safety and the protection of our values. Hereafter, the 'digital rulebook' or 'digital rules' are understood broadly as the body of EU legislation with a significant digital angle and its implementation. Examples include, but are not limited to, rules on data, artificial intelligence, telecommunications services, regulations on online platforms and digital services, media services, cybersecurity or privacy of communications.

For businesses and organisations:

How has the EU's digital rulebook created opportunities or otherwise positively impacted your business?

Identify the 3 pieces of EU regulation holding a digital angle that have had the largest impact on your organisation. This will inform the European Commission's scoping and prioritisation of the legal framework to be analysed more in-depth in the Digital Fitness Check. If you are not familiar with the names of specific legislative acts, you may refer instead to policy areas or domains.

For all respondents:

What do you consider to be the most important achievements of the EU-wide digital rulebook? Please explain.

What are the benefits for cross-border trade within the EU supported by the application of digital legislation?

- [ ] Increased market access
- [ ] Regulatory consistency
- [ ] Legal certainty

- Access to EU digital infrastructures
- Competitive pricing
- Rights protection
- Enhances safety and quality
- Increased innovation
- Other

Please explain your experience related to the previous question and/or elaborate on 'Other'.

What are the benefits for cross-border trade with non-EU countries supported by the application of digital legislation?

3. Challenges and areas where further analysis and optimisation of the rules are needed

The Draghi and Letta reports highlight that the accumulation of rules has sometimes had an adverse effect on competitiveness. Fast and visible improvements are needed for people and businesses, through a more cost-effective and innovation-friendly implementation of our rules – all the while maintaining high standards and core objectives of the rules.

The first step is a 'stress-test' of the rules, to see their real-world impact, not just in isolation, but in the way they are applied together by businesses, administrations and other organisations, and how they achieve their goals.

Based on the preliminary views received from stakeholders on the margins of the consultations for the Digital Omnibus, there is a need for a wider analysis on the interplay between laws for example as regards the data acquis of the EU, or more recent rules applicable to cybersecurity or to online services and sector-specific rules.

What are, in your opinion and experience, areas of digital law where there is scope for making key improvements? Be as precise as you can. Please highlight, where possible, the aspects specifically relevant to SMEs.

Credit information suppliers believe there is scope to make key improvements in the GDPR and the EU AI Act – both individually and in terms of their interplay with each other and with sector-specific legislation such as the

revised Consumer Credit Directive (CCD2).

Our sector is heavily impacted by digital law. In a paper published by the Journal of Banking Regulation by Dr. Judith Arnal, a member of the Governing Board of the Bank of Spain, the rules and requirements concerning credit scoring are characterised as a 'legal maze' [reference: Arnal, J. Unfit for purpose? The legal maze of credit scoring under EU law. J Bank Regul 27, 14 (2026). https://doi.org/10.1057/s41261-026-00311-7]. Furnishing a credit score is touched upon by inter alia the EU AI Act, GDPR and the revised Consumer Credit Directive.

Article 22 GDPR – Automated Decision-Making

ACCIS was encouraged by the European Commission's proposals to amend Article 22 of GDPR via the Digital Omnibus. Like many industry bodies ACCIS has long-held the view that there has been a wide discrepancy between the original intent of the law and how it has been enforced and interpreted. Of special relevance to credit scoring is Article 22 on Automated Decision Making. It is our view that if Article 22 is not addressed through the Digital Omnibus then it should be addressed by any proposals in the Digital Fitness Check.

Since the Court of Justice of the EU's ruling in case C-634/21 in December 2023 it has been the case that an automated credit score, when used decisively in lending decisions, qualifies as automated decision-making under Article 22(1) of the GDPR. Unless specific exceptions apply – such as a law at National-level or if it is necessary for entering into, or performance of, a contract between the data subject and a data controller – this type of processing is prohibited. We urge policy makers to provide guidance on what constitutes a decisive decision, as well as recognition of the reality that credit information suppliers provide a credit score as a 3rd party to a borrowing transaction between lender and consumer. There may be situations in which companies fall within the scope of Article 22 GDPR if they rely significantly on automatically determined values or assessments when making a decision that has a significant impact on the data subject. In such cases, the question arises as to whether it is consistent that the one making the decision benefits from exception under Article 22(2)(a) GDPR, while a third party who has created this automated assessment and who, according to the case law of the ECJ, may therefore fall within the scope of Article 22 of the GDPR, has fewer options to deviate from the prohibition of Article 22(1) GDPR if this exception is interpreted narrowly.

Codes of Conduct

Amending GDPR should also strengthen the role of Codes of Conduct ('CoC'; Articles 40 and 41 GDPR). CoCs enable industries and sectors to develop practical and context-specific guidelines and offer members legally compliant guidance. An approved CoC can serve as proof of compliance (Art. 24(3) GDPR) and thus promote legal certainty. For instance, it could be proposed to amend Article 82 GDPR in order to reduce fines and claims for damages for those companies that follow approved CoCs.

EU AI Act – Definition of AI System

On the AI Act, one key improvement would be for the Commission to clarify definitively that logistic regression does not constitute an AI system within the meaning of the Act. This would be consistent with the intention of the legislation and is supported by the European Central Bank. Absent this clarification, standard and well-established statistical tools risk being swept into a high-risk compliance regime designed for genuinely novel AI systems, creating disproportionate burden without commensurate benefit to consumers or financial stability.

Cross-cutting: Digital Distribution and AI-Driven Credit Scoring

There is also a broader point about the reality of lending decisions in a digital distribution model, where decisions to grant or deny credit are made increasingly in automated environments. This makes the automated

decision-making provisions of both the GDPR and the AI Act increasingly central to our sector's operations. A key improvement would therefore be a more consistent and proportionate treatment of credit scoring across EU digital laws, one that takes into account its nature and role in responsible lending and its contribution to financial stability.

To what extent do you perceive overlaps, conflicts, or redundancies between the EU digital legislation and sector-specific EU regulations in your area of activity? Please provide examples and elaborate on aspects you find problematic.

As referenced in the question above, there exist some overlaps, conflicts and redundancies between EU digital legislation and financial services law.

Example 1: the EU AI Act mandates risk and quality management in Articles 9 & 17, which credit information suppliers must comply with in the event they are using AI-driven credit scoring. Financial services sector legislation already requires comprehensive internal control frameworks.

Example 2: as illustrated by Arnal (2026), the European Court of Justice (ECJ) landmark ruling in Case C-634 /21 which ruled that the automated establishment of repayment probabilities by third-party credit information suppliers, when used decisively in lending decisions, constitutes automated decision-making under Article 22 (1) of the GDPR. Unless specific exceptions apply (contractual necessity, consent, national law), such processing is prohibited. That is complicated further because under the AI Act, AI systems used to assess the creditworthiness of natural persons are high-risk, triggering extensive compliance obligations, but not prohibiting. Furthermore, credit scoring remains simultaneously subject to existing financial regulation and consumer protection rules under the Consumer Credit Directive and Mortgage Credit Directive. This is a multi-layered regulatory framework where data protection, AI governance, and sectoral financial rules intersect—often without clear coordination mechanisms. Reference: Judith Arnal, 2026. "Unfit for purpose? The legal maze of credit scoring under EU law," Journal of Banking Regulation, Palgrave Macmillan, vol. 27(2), pages 1-11, June.

Moreover, the credit sector is already governed by a robust and mature regulatory framework that addresses many of the risks horizontal digital legislation aims to mitigate. There are overlaps between horizontal digital legislation and established rules in:
• Financial Services Law: Prudential regulations like CRD IV and Solvency II, along with EBA Guidelines, already mandate comprehensive risk and internal control frameworks that overlap with the AI Act's requirements for risk management (Art. 9), quality management (Art. 17), and post-market monitoring (Art. 19).
• Data Protection Law: The General Data Protection Regulation provides a strong foundation for data governance, human oversight of automated decisions, transparency, and impact assessments (DPIAs), which directly intersect with the AI Act's obligations, such as data governance (Art. 10), human oversight (Art. 14), transparency (Art. 13), and impact assessments (Art. 27).
• Consumer Protection Law: The Consumer Credit Directive 2023/2225 (CCD2) already grants consumers the right to a human review and a “clear and comprehensible explanation” for creditworthiness assessments (Art. 18(8) CCD2), mirroring the objectives of the AI Act’s transparency and human oversight provisions.
• Cybersecurity Law: Legislation such as DORA, NIS2, and the Cyber Resilience Act (CRA) imposes detailed cybersecurity obligations on businesses in various sectors, which overlap with the cybersecurity requirements in Art. 15 AI Act.

To what extent do you perceive overlaps, conflicts, or redundancies between the EU's digital rules and legislation issued by Member States? Please provide examples.

On GDPR, we first acknowledge that proposed amendments have been tabled in the Digital Omnibus package. That being said, ACCIS – like many other organisations – has observed fragmentation across EU Member States regarding the legal basis for processing data (i.e Article 6).

We urge policy makers to provide guidance on what constitutes lawful grounds for data processing based on legitimate interest, as we see different interpretations within Member States. We acknowledge various initiatives proposing non-exhaustive list for legitimate data processing activities that provide clear guidance for companies. These legitimate data processing activities should include activities that are performed prior to entry into transactions that carry a financial risk of default, such as creditworthiness checks, fraud prevention, legitimacy checks, money laundering prevention, identity and age checks, address identification, customer service or risk management as well as setting rates and conditions

In addition, if we look into Article 22, pertaining to Automated Decision Making, exceptions allowing ADM, subject to appropriate safeguards can be through an authorisation in Member State Law through Article 22(2)(b). This exception is necessary, since Member States treat credit scoring differently in what pertains to the legal basis for processing data: some countries (Italy) have codes of conduct, others rely on legitimate interest, whereas others rely on public interest.

Are there EU rules or provisions in the digital area that you believe are no longer up to date, or that are obsolete?

The absence of common EU-level tools and standards for pseudonymisation and anonymisation represents a significant gap. Without shared technical and legal criteria for what constitutes effective pseudonymisation, privacy-enhancing technologies are difficult to deploy with legal certainty, and the resulting data – even when technically protected – may be too limited in utility to support accurate credit modelling.

This gap has direct single market consequences: credit information suppliers operating cross-border cannot rely on consistent rules for when pseudonymised data falls outside the scope of the GDPR, creating compliance asymmetry and inhibiting legitimate data sharing. The Digital Omnibus proposals on pseudonymisation are a step in the right direction, but they should be accompanied by practical guidance developed in partnership with industry and the EDPB, rather than left to implementing acts alone.

Regarding cross-border trade within the EU, what negative effects do you experience (if organisation, within your sector) from the application of digital EU legislation?

- ☐ Increased compliance costs
- ☐ Regulatory fragmentation
- ☐ Reduced innovation capacity
- ☐ Market concentration
- ☐ Slower market entry

- [ ] Limited consumer choice
- [ ] Other

Please specify your answer to the previous question.

What are possible negative consequences of the application of digital EU legislation for cross-border trade with non-EU countries?

Based on the preliminary views received on the margins of the consultations for the Digital Omnibus, stakeholders pointed to the need for a more in-depth analysis of elements such as:

- The coherence between specific legal notions, such as definitions, or questions of clarity of obligations and coherence of scope;
- The cumulative impact of rules and potential for further streamlining, in particular where there are duplications of obligations;
- The good practices and challenges in the interplay between the different governance systems of the rules, including cooperation and consultation mechanisms between authorities and EU-level cooperation through Boards and other fora;
- Mechanisms, tools, guidance or experimental practices that bring legal clarity, burden relief or assist in the application of rules in novel areas, supporting innovative practices.

The questions below seek to collect your views on these elements and invite you to reflect further on other areas that could require further analysis. Your replies will inform the Commission in scoping the analysis for the Digital Fitness Check.

What areas, if any, do you perceive as incoherent and unclear in terms of concepts used across different laws, definitions, or scope of the rules?

The definition of "AI system" under the AI Act was clarified under the Guidelines of February 2025, which confirmed that long-established statistical techniques – such as standalone logistic regression models (i.e. models that do not combine with, or incorporate, AI elements in their development or use) – fall outside the scope of AI systems. These models have been used safely in financial services for over 50 years, with no evidence of consumer harm. During this implementation period, however, there is currently uncertainty about how to operationalise the guidelines, with unclear interpretation of AI systems across Member States, so ensuring legal certainty on the definition of AI across the Single Market matters significantly for credit information suppliers: if logistic regression is treated as an AI system, models that have been in lawful and responsible use for decades are potentially subject to the high-risk regime under Annex III, with associated documentation, conformity assessment and human oversight obligations. We call on the Commission to provide a definitive, legally binding clarification that logistic regression does not fall within the definition of an AI system, consistent with the Act's underlying intent.

In what areas, if any, do you consider that changes could be made to optimise the cumulative impact of the rules? In particular, where do you identify, in practice, that obligations in different rules lead to duplications of costs or processes?

Technically, it is still to be played out but we assess the documentation requirements of the EU AI Act for High-Risk systems e.g. under Article 11 to be onerous. Requirements should be as practical as possible and take into account bureaucracy and compliance burdens that European companies already face today.
In order to avoid overarching bureaucracy the data protection impact assessment (Art 35 GDPR) and the fundamental rights impact assessment (AI Act Art. 27) should be linked and thought together.

You can find as an Annex to the Staff Working Document supporting the Digital Omnibus proposal a detailed list of **reporting obligations** identified across major digital EU legislation, including one-off obligations, as well as recurrent reporting requirements.

The Commission has already made proposals for streamlining reporting obligations, for example through the **Digital Omnibus** proposal for cybersecurity and related incident reporting, and for online platforms, with the repeal of the Platform-to-Business Regulation.

In addition to these immediate changes, stakeholders have flagged **other areas** where further streamlining across different horizontal and sector-specific requirements could facilitate their business operations, for example as regards reports on content moderation decision or risk assessments.

Are there areas of digital law where you currently identify a disproportionate administrative burden stemming from reporting obligations?

Technically, it is still to be played out but we assess the documentation requirements of the EU AI Act for High-Risk systems e.g. under Article 11 to be onerous. Requirements should be as practical as possible and take into account bureaucracy and compliance burdens that European companies already face today.
In order to avoid overarching bureaucracy the data protection impact assessment (Art 35 GDPR) and the fundamental rights impact assessment (AI Act Art. 27) should be linked and thought together.

What reporting obligations are particularly important for transparency and accountability in the sector you are active in?

In November 2025, the European Banking Authority completed a comprehensive mapping exercise examining how AI Act obligations interact with existing EU banking and payments regulation for creditworthiness assessment and credit scoring systems. The EBA's analysis confirms that substantial overlaps exist between AI Act requirements and sectoral frameworks such as the CRR/CRD, Consumer Credit Directive, Mortgage Credit Directive, DORA, and the EBA's own Guidelines on Loan Origination and Moni¬toring (see here: https://www.eba.europa.eu/sites/default/files/2025-11/2019d1b5-59f8-4149-ad3b-23cfcd4388a1/EBA%20Chair%20letter%20to%20Mr%20Berrigan%20and%20Mr%20Viola%20on%20outcome%20of%20EBA's%20AI%20Act%20mapping%20exercise.pdf).

If you are the recipient of reports from businesses or other entities, what are the possibilities for rendering more efficient the forms and ways in which you receive the reports?

4. Governance models

What are the good practices you have identified in the governance structure applicable to digital rules? Do you see particularly notable success stories for example when it comes to the cooperation across authorities, coordination in enforcement actions, clarifications and support actions for assisting businesses, organisations and consumers in the application of the rules?

What challenges do you identify in the governance structures of the digital rules?

5. Beyond the letter of the law: models that support the application of the rules

What are good examples of supporting actions and experimental practices that can help in giving legal clarity, cutting compliance costs, or supporting innovative practices and the take-up of new technologies, in particular for SMEs?

One-click compliance

Supporting actions do not come only from authorities, but private entities also provide new mechanisms of assistance. In the Communication on a Data Union Strategy, the Commission explored in particular the concept of 'one-click compliance', where regulated entities can delegate compliance tasks, where this is permissible, to certified third-party providers. Such models can bring considerable optimisations, ensuring at the same time that the objectives of the rules are fully achieved.

Not all legal obligations can be prone to such mechanisms, and the important legal questions on liability and oversight arise. Determining who is accountable in case of errors, misuse, or system failures - whether the company, the certifier, or the regulator - will be essential to ensure trust and legal certainty.

What are sectors where such a 'one-click compliance' mechanism can bring particularly important opportunities? Please explain.

How could such mechanisms in conjunction with solutions like the European Business Wallets or the Digital Product Passport aid in enhancing trust, creating opportunities and simplify compliance?

How do you currently manage compliance with EU digital or data-related legislation? Do you rely on external systems or resources? Please explain.

Would digital tools that automate certain compliance tasks be useful for your organisation? If yes, in which areas?

What would you need to trust such solutions (e.g. certification, legal clarity, public oversight)?

What risks or concerns would you see in using automated compliance tools?

How could the EU best support their safe and effective use (e.g. standards, guidance, funding, pilots)?

6. Closing section

Please share any other remarks that you find important for the Commission to take into account in conducting the Digital Fitness Check. Please share any evidence, data, practical examples and analysis.

You may attach an additional document here:

Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

Contact

CNECT-DIGITAL-SIMPLIFICATION@ec.europa.eu