

Position Paper: Digital Networks Act

Executive summary

FEDMA welcomes the Digital Networks Act proposal, and particularly the objective of simplifying and further harmonising the legal telecommunications framework to strengthen the internal market. However, the transfer of some ePrivacy Directive provisions to the Digital Network Act (**DNA**) risks leading to (unintended) spillover effects, legal inconsistencies and legal uncertainty, which will negatively impact the internal market and economic growth for businesses, particularly SMEs. It will also limit fundraising and other activities of NGOs and charities.

While the DNA transfers selected ePrivacy provisions into the new framework, Article 12 of the ePrivacy Directive governing publicly available directories is not replaced by any operative provision and is addressed only in recital 307. Moreover, the “conflict of law clause” in the recital creates more legal uncertainty regarding the legal framework applicable to directory inclusion than it prevents it. The recital also risks introducing a *de facto* consent-based model through recital language alone. This will have a significant negative impact on individuals, businesses, SMEs, charities and NGOs who continue to rely on publicly available directories to find and contact relevant persons efficiently.

Furthermore, recital 307 misattributes fraud risk to publicly available directories based on opt-out models. There is limited evidence that opt-in and opt-out directory frameworks are a determining factor in fraudulent activities, particularly because fraudulent actors typically rely on amongst other information harvested from social media (rather than directories). Crucially, other policy options have proven successful in preventing fraudulent activities.

Finally, the DNA should preserve a clear distinction between directory inclusion rules, telemarketing regulation and fraud-prevention measures. Undefined concepts, such as “nuisance calls”, risks leading to legal uncertainty and risks limiting several legitimate telemarketing companies.

Key recommendations:

- Introduce a dedicated operative provision on publicly available directories (Article 107a) following an opt-out model.
- Amend recital 307 to ensure that it fulfils its interpretative function, uses precise terminology which accurately reflects operational realities and the purpose of publicly available directories. Substantive obligations should also be left to operative text.
- Clarify the concept of “nuisance calls” through a dedicated definition in the Digital Network Act.
- Address fraud risks through proven caller-authentication, anti-spoofing and caller-verification measures rather than restrictions on directory inclusion and telemarketing.

Contents

1. The DNA should seamlessly complement existing EU legislation without creating legal uncertainty or unintended regulatory spillover effects.....	3
1.1. A clear distinction between the DNA and ePrivacy must be preserved	3
1.2. Directory inclusion should not depend on the variable qualification of contact details as personal data.....	4
1.3. Undefined concepts should not create unintended regulatory spillover effects.....	5
2. Publicly available directories remain an essential enabler of legitimate communications and telemarketing	6
3. The DNA should establish a legal framework for publicly available directories based on an opt-out model.....	8
4. Fraud should be addressed through targeted anti-spoofing and caller authentication measures	9
5. Measures that mainly constrain compliant actors are unlikely to reduce fraud while potentially harming SMEs, charities and consumers	10

1. The DNA should seamlessly complement existing EU legislation without creating legal uncertainty or unintended regulatory spillover effects

As presented by the European Commission, the DNA's proposal aims to simplify and further harmonise the legal framework in order to strengthen the internal market and should therefore be interpreted and applied in a manner that complements existing legislative frameworks and promotes regulatory coherence.

1.1. A clear distinction between the DNA and ePrivacy must be preserved

As explicitly stipulated in the DNA proposal, the integration of *some* provisions, including from the ePrivacy Directive, into the DNA (i.e. Articles 108, 109 and 110) aims at meeting the above-mentioned objectives.¹ Articles 108 and 109 DNA provide for caller identification requirements and allow restrictions on the display of caller identification to be overridden for the purpose of tracing “nuisance calls”. In addition, Article 110 DNA allows for limiting the reception of nuisance calls at the request of the end user.² The provisions transferred from the ePrivacy Directive to the DNA aim at enhancing transparency, privacy, traceability, and user control over phone calls.³

One provisions from the ePrivacy Directive is not transferred into any DNA operative provision and remains only mentioned in the recitals: Article 12 on the directories of subscribers is only transferred to recital 307. This DNA recital misattributes fraud risks to opt-out models which would be permitted by Article 12 of the ePrivacy Directive. Recital 307 DNA:

- Improperly frames opt-out directory models negatively, suggesting that allowing individuals to object to inclusion or withdraw consent “may lower the level of protection” and “expose end-users to fraudulent practices by malicious actor”; and
- Stipulates that consent should always be required before including natural persons in directories, explicitly endorsing a pure opt-in model.

There is currently limited evidence that the choice between opt-in and opt-out directory frameworks is a determining factor in the success of fraudulent activities.⁴ Besides, while recital 307 explains why mandatory directory services may no longer be necessary in light of digital alternatives, it is less clear why this should lead to the introduction of a harmonised consent-based model for directory inclusion, particularly where no corresponding operative provisions are proposed.

Apart from the ePrivacy provisions that are intended to be moved to the DNA, the remaining provisions of the ePrivacy Directive remain in place, and the rights, obligations and policy choices

¹ Recital 4 and Article 207 DNA.

² This provision applies next to Article 97 of the European Electronic Communications Code which stipulates that, in principle, Member States must provide access to all numbers in the EU.

³ Recitals 301-305 DNA.

⁴ For instance: Ofcom (British telecom regulator), Study on “Joint online, calls and texts fraud research” (2024), [weblink](#).

reflected therein should be preserved in the interest of legal certainty. As a matter of fact, Article 13 ePrivacy Directive (which governs the conditions under which direct marketing calls and other electronic communications may be made) was not transferred to the DNA. Therefore, the applicable opt-in and opt-out telemarketing rules and safeguards available to individuals will fall within the scope of the ePrivacy Directive. As those provisions remain in force, the DNA should be interpreted and applied consistently with the ePrivacy framework to preserve legal certainty and avoid regulatory fragmentation.

FEDMA recommends deleting the following in recital 307:

~~“Sometimes, Member States provide that end-users have the right to object the inclusion of their personal data in their national laws or the withdrawal of consent of a natural person is not shared with third parties processing personal data from the directories, which may not only lower the level of protection throughout the Union, but also expose end-users to fraudulent practices by malicious actors.”~~

1.2. Directory inclusion should not depend on the variable qualification of contact details as personal data

Furthermore, as several recitals and provisions of the DNA recognise, the GDPR remains *the primary framework* governing the processing of personal data. For instance, Article 2(50) DNA refers to the definition of ‘consent’ under the GDPR for the purposes of applying the DNA.

Recital 307 is imprecise in its formulation when explicitly stating that the aim of a directory is to enable identification of persons. The primary function of publicly available directories is to facilitate communication by making contact details searchable and accessible. The recital therefore appears to be based on the incorrect assumption that directory services are primarily intended to identify individuals, whereas in practice they are intended to enable users to find and contact relevant persons, businesses and other organisations. Besides, referring to the "identification" of persons risks conflating the operational purpose of directories with the distinct data protection concept of identifiability, thereby creating unnecessary legal uncertainty.

FEDMA recommends modifying recital 307 as follows:

~~“The main function of directory services is to enable users to identify such persons find and contact natural and legal persons through their contact details.”~~

Besides, the GDPR only applies to the processing of personal data, and recent national case law has confirmed that telephone numbers do not automatically constitute personal data in all

circumstances.⁵ This decision is aligned CJEU caselaw.⁶ As a result, the applicability of the GDPR may differ depending on circumstances and the interpretation adopted by national courts and national data protection authorities.

Yet, recital 307 stipulates that consent for inclusion in a directory should be obtained in accordance with the GDPR. Where a telephone number or other contact details do not constitute personal data in a particular context, it becomes unclear whether the GDPR-based consent requirement applies at all and, if not, which legal framework governs inclusion in the directory? In the absence of a corresponding operative provision in the DNA, this will result in divergent interpretations across Member States and create legal uncertainty not only for directory providers and end-users, but also for SMEs, NGOs and other legitimate users of directory services which rely on publicly available directories to identify and contact relevant individuals.

FEDMA recommends deleting the following in recital 307:

■ ~~“Furthermore, it is appropriate for ensuring a high level of protection of the right to privacy and to protection of the personal data that end-users who are natural persons are asked for consent before their personal data are included in a directory.”~~

~~[...]~~

■ ~~“Requesting consent, including for sharing contact details in an electronic or paper form irrespective of the provider should be in accordance with Regulation (EU) 2016/679.”~~

1.3. Undefined concepts should not create unintended regulatory spillover effects

Care should also be taken to ensure that the concepts introduced by the DNA do not inadvertently affect the interpretation of other regulatory frameworks because regulatory concepts developed for one purpose often influence adjacent areas of law and policy pursuing different objectives. There is therefore concern about the potential impact of some DNA provisions (or the lack thereof) on the future interpretation of marketing and data protection rules.

In particular, the concept of "nuisance calls" remains undefined and should not become a basis for restricting lawful and legitimate communications. The understanding of what constitutes a nuisance call may differ significantly between industry, policymakers and enforcement

⁵ For instance, in its judgment of 15 May 2025 (III OSK 6555/21), the Polish Supreme Administrative Court held that a telephone number does not automatically constitute personal data under Article 4(1) GDPR and that, where a number cannot reasonably be linked to an identifiable individual through available additional information, its processing falls outside the scope of the GDPR (weblink [here](#)).

⁶ C-413/23 EDPS v. SRB, C-582/14 Breyer.

authorities. Without clear safeguards, there is a risk that legitimate commercial and charitable communications could gradually become associated with a broader and vague category of undesirable communications. Therefore, to ensure legal certainty, a clear distinction should therefore be maintained between abusive or fraudulent communications, and communications that are lawfully carried out in accordance with applicable EU or national legislation, including Article 13 of the ePrivacy Directive.

FEDMA recommends adding the following definition of “nuisance calls” to Article 2 of the DNA proposal:

"Nuisance calls" should mean repeated or persistent communications objectively causing significant disturbance to end-users, including silent, abandoned or excessive automated calls, without prejudice to communications lawfully made under Union or national legislation. A communication should not be considered a nuisance call solely on the basis of its commercial or marketing nature where it complies with the applicable Union or national rules governing direct marketing.

2. Publicly available directories remain an essential enabler of legitimate communications and telemarketing

Publicly available directories play a vital role in enabling individuals, companies, and NGOs to identify and reach the right people efficiently, supporting essential functions such as customer service, identity verification, and charitable outreach. For many organisations, particularly SMEs and non-profit entities, directories represent an accessible and cost-effective means of establishing initial contact with potential or already existing customers, donors or stakeholders.

Beyond their role in enabling businesses and organisations to reach individuals, publicly available directories also serve an important protective function for consumers themselves. Individuals frequently rely on publicly available directories to cross-check the identity of a company or individual they are dealing with — for example, verifying that a stated business address, registered name or telephone number genuinely corresponds to the entity or person they are engaging with. This form of independent, user-initiated verification helps consumers detect impersonation, fictitious businesses or misrepresented identities before entering into a transaction or communication. Preserving broad and accurate directory coverage therefore directly supports consumers' own ability to protect themselves, complementing — rather than substituting for — the targeted anti-spoofing and caller-authentication measures discussed below (ref. [section 4](#)), which address fraud at the level of the communications infrastructure itself.

Publicly available directories also form part of the wider ecosystem on which lawful telemarketing relies. Access to accurate and up-to-date contact information enables businesses to reach potential customers, inform them about products and services, and compete effectively in the marketplace. Limiting the availability of directory data may therefore have consequences that extend beyond directory providers themselves and affect the ability of legitimate organisations to communicate with interested individuals.

At the same time, publicly available directories contribute to consumer choice and market competition by lowering barriers to communication between companies and potential customers. Where significantly fewer contact details are available through directory services, businesses may face greater difficulties in reaching new customers, particularly in sectors that rely on direct channels of communication. Such outcomes will also disproportionately affect SMEs and charities, which often lack the resources and brand recognition available to larger market participants.

Furthermore, as highlighted in FEDMA's recent comparative analysis of telemarketing regulation across Member States, there is no robust evidence that opt-in models inherently provide a higher level of consumer protection than opt-out models. The effectiveness of telemarketing regulation depends on a broader set of factors, including enforcement, consumer awareness and the national regulatory context.⁷ Consequently, reducing the availability of directory information through a mandatory opt-in model should not be assumed to deliver corresponding consumer-protection benefits.

Moreover, recital 307 assumes that online search engines, social media platforms and online directories have replaced the role traditionally fulfilled by publicly available directories. This assumption overlooks that the availability of online contact information frequently depends on the existence of directory data in the first place. Much of the information now discoverable online has historically been collected, verified, structured and made accessible through directory services. Digital alternatives should therefore be seen as complementary channels within the same ecosystem, rather than as evidence that publicly available directories no longer serve a useful purpose.

For these reasons, the existing ePrivacy regulatory framework governing publicly available directories should seek to preserve their societal and economic value while ensuring that end-users retain effective and meaningful control over their contact details.

FEDMA recommends modifying recital 307 as follows by adding the sentence in bold and deleting the strikethrough text below:

"The increasing availability and use of digital alternatives like online search engines, social media and online directories that offer an up-to-date way to find contact

⁷ FEDMA (June 2026), Regulating Telemarketing in the EU: An Evidence Based and Comparative Analysis with a Focus on Opt-In and Opt-Out Frameworks (available [here](#)).

*information do not justify maintaining the obligation on number-based interpersonal communications services providers rely on and complement the wider well-established directory systems. **Publicly available directories continue to fulfil important functions for individuals, businesses and organisations and should therefore remain subject to a clear and predictable legal framework.***

3. The DNA should establish a legal framework for publicly available directories based on an opt-out model

While the DNA proposes to transfer selected provisions of the ePrivacy Directive into the new framework, Article 12 of the ePrivacy Directive, which governs directories of subscribers, is not reflected in any operative provision of the DNA. Instead, the subject is addressed only in Recital 307. Given the continued importance of publicly available directories and the proposal's objective of promoting legal certainty and harmonisation, the DNA should contain a dedicated operative provision establishing a clear framework for the inclusion of contact details in publicly available directories.

By contrast, a mandatory opt-in approach is likely to result in significantly fewer directory listings, thereby reducing the usefulness of directory services for consumers, businesses and organisations. Diminished directory coverage may also affect lawful telemarketing activities, customer acquisition efforts and the ability of SMEs and charities to reach new audiences. In practice, such outcomes may reduce consumer choice, limit opportunities for legitimate communication and increase barriers for smaller organisations seeking to compete with more established market participants.

Finally, the framework governing directory inclusion should apply irrespective of whether a particular telephone number or contact detail qualifies as personal data in a specific context. As demonstrated by recent case law, the qualification of a telephone number as personal data may depend on the circumstances of the processing and the ability of the controller to identify the individual concerned.

FEDMA recommends adding the following provision within the DNA:

Article 107a

Publicly available directories and directory enquiry services

1. This Article applies to publicly available directories and directory enquiry services containing contact details of end-users, including phone numbers, mobile phone numbers, email addresses.

2. The inclusion of contact details in publicly available directories shall be permitted provided that the end-user concerned is informed, free of charge, before inclusion, of:

(a) the purpose or purposes of the publicly available directory; and

(b) any further usage enabled by the directory, or directory enquiry service.

3. End-users shall have the right, free of charge and at any time, to object to the inclusion of their contact details in a publicly available directory, and to determine which of their contact details are included in the directory, to the extent that those contact details are relevant for the purpose of the directory.

4. The inclusion of contact details in a publicly available directory for the purpose of enabling the search of contact details on the basis of a name and, where necessary, a minimum of other identifiers shall not require prior consent, provided that the safeguards set out in this Article are complied with.

5. End-users shall have the right, free of charge, to verify, correct, delete or withdraw such contact details.

6. The legitimate interests of end-users other than natural persons with regard to their inclusion in publicly available directories shall be sufficiently protected.

7. This Article shall be without prejudice to Regulation (EU) 2016/679 and to Union or national rules governing unsolicited communications, including Article 13 of Directive 2002/58/EC.

4. Fraud should be addressed through targeted anti-spoofing⁸ and caller authentication measures

The proposed justification for a mandatory opt-in model in recital 307 appears to conflate two distinct policy objectives:

- (i) the governance of publicly available directories and
- (ii) the prevention of fraud.

Historically, directory inclusion rules have been designed to give individuals control over the publication and accessibility of their contact details while preserving the utility of directory services and have not served as anti-fraud mechanisms. A clear distinction should therefore be

⁸ Spoofing is a deceptive practice where a malicious actor disguises or falsifies communication data (such as a phone caller ID) to impersonate a trusted entity, company or person in order to trick victims and commit fraud. Source: Europol (2025), Position Paper on Caller ID Spoofing, available [here](#).

maintained between measures governing directory inclusion and measures aimed at combating spoofing, deceptive communications and other fraudulent activities.

There is limited evidence that the choice between an opt-in and an opt-out model for publicly available directories is a determining factor in the success of fraudulent activities. Fraudulent actors typically rely on spoofed caller identities, misleading communications and data obtained through a variety of channels rather than on publicly available directories. Consequently, restrictions on directory inclusion should not be presented as a primary fraud-prevention measure where the underlying risks arise from different sources.

Moreover, publicly available directories continue to fulfil important societal and economic functions. They facilitate customer service, identity verification, charitable outreach and lawful communications between individuals, businesses and organisations. A mandatory opt-in system would likely reduce the availability of directory information, thereby negatively affecting legitimate users while having little limiting impact on actors engaged in fraudulent activities.

Rather than restricting directory inclusion, the DNA should focus on targeted measures that directly address fraud. The proposal already includes provisions enabling caller identification, tracing of malicious or nuisance calls and blocking of specific or anonymous calls. In addition, Europol has highlighted the importance of caller-authentication and caller-verification solutions capable of detecting spoofed identities and tracing fraudulent communications.⁹ The EU could further explore proven technical solutions, such as STIR/SHAKEN-type caller authentication frameworks. Such measures address the root causes of fraud more directly and effectively than restrictions on publicly available directories.

In Spain, a Responsible Communications Registry is being set up, which is an industry-led (by Adigital) caller authentication solution. It enables companies and contact centres to register and validate telephone numbers, improving transparency, traceability and the recognition of legitimate calls by operators and consumers. As such, the initiative helps to distinguish lawful and legitimate calls from fraudulent or spoofed calls. Such practical solutions illustrate the type of caller-authentication and verification measures that the DNA should encourage, as they address the root causes of fraud and spoofing directly while avoiding unnecessary restrictions on legitimate and lawful calls and publicly available directories.

5. Measures that mainly constrain compliant actors are unlikely to reduce fraud while potentially harming SMEs, charities and consumers

As recognised in the DNA proposal itself, the communications ecosystem is evolving, and individuals increasingly rely on digital alternatives such as search engines, social media platforms and online directory services to identify and contact one another. Recital 307 even questions whether the traditional obligation to maintain publicly available directories remains necessary in light of these developments. However, the growing role of digital alternatives should

⁹ Europol (2025), Position Paper on Caller ID Spoofing, available [here](#).

not automatically be interpreted as a reason to reduce the availability of directory information or to restrict access to legitimate communication channels.

Indeed, a mandatory opt-in approach would primarily affect compliant actors that operate within the regulatory framework, including directory providers, charities, SMEs and legitimate marketing organisations. Fraudulent actors typically do not rely on publicly available directories to obtain contact data and do not generally comply with regulatory obligations governing directory inclusion. As a result, measures restricting the availability of directory information are unlikely to have a significant impact on fraud while directly affecting organisations that lawfully use directory data for customer service, prospecting, charitable outreach and identity verification.

The practical effect may therefore be a reduction in the amount of reliable and accessible contact information available to legitimate market participants. This may be particularly problematic for SMEs and non-profit organisations, which often lack the resources, brand recognition and proprietary datasets available to larger organisations. Reduced access to directory information may increase barriers to reaching new customers, donors and stakeholders, thereby limiting opportunities for growth, competition and innovation.

Furthermore, if publicly available directories become less comprehensive, organisations may increasingly have to rely on alternative sources of contact information provided by large digital platforms, online search engines and social media services. This could further concentrate access to contact and visibility data in the hands of a limited number of digital gatekeepers. In practice, resources and business opportunities may shift away from SMEs, charities and specialised European data-driven marketing providers towards larger platform operators that control access to audiences and contact information.

Such an outcome would neither address the underlying drivers of fraud nor contribute to a competitive and diverse communications ecosystem. Policymakers should therefore ensure that measures intended to improve user protection target fraudulent behaviours directly, while preserving the ability of legitimate organisations to communicate with individuals through transparent and accountable channels.
