November 2020

Non-Paper of the German Federal Government
on the Digital Services Act Package

The Federal Government has commented in detail on the public consultation of the European Commission (COM) on the Digital Services Act (DSA) Package. The Federal Government welcomes the initiative of the COM to review Directive 2000/31/EU of 8 June 2000 on electronic commerce (e-Commerce Directive) within the framework of the DSA and to create better rules on responsibility and security for digital platforms, services and goods, to strengthen the internal market for digital services and to help smaller companies achieve legal clarity and a level playing field. In regulating large platforms with a gatekeeper function, the Federal Government advocates a combination of directly applicable general rules of conduct and bans on certain practices ('blacklisted practices') with more far-reaching remedies to be imposed by the competent authority in individual cases.

In summary, the Federal Government takes the following positions:

A. Review of the e-Commerce Directive

The horizontal legal framework for digital services has remained unchanged since the adoption of the e-Commerce Directive. At the time, the Directive harmonised the relevant basic principles and made it possible for services to be provided cross-border. It has since then served as the cornerstone for regulating digital services in the European Union (EU). Progressive digitisation is now expanding the range of digital services on offer. In the 20 years since the adoption of the e-Commerce Directive, the digital economy has developed dramatically and at a rapid pace. The digital transformation is having a key impact on citizens' lives, in terms not only of the goods and services on offer, but also of the expansion of public space to include private-sector digital platforms. It is crucial that the EU pursues a 'European approach' to digitisation. In addition to strengthening the internal market from a business perspective, the aim today is also to make it trustworthy for consumers and to protect our democracies under the rule of law.

In the COVID-19 pandemic, the great potential of digital solutions for the common good and to support citizens has become even clearer. At the same time, however, gaps, shortcomings and risks have also become apparent. Platforms should therefore be obliged to take more measures to protect their users. The position of consumers vis-à-vis online networks needs to be strengthened. There also needs to be a level playing field between providers from the internal market and from non-European countries.

The Federal Government therefore welcomes the Commission's initiative to review the e-Commerce Directive within the framework of the DSA. Across all of the provisions, care should be taken to ensure that small and medium-sized (European) providers are not unduly burdened. It

needs to be possible for more stringent obligations to be imposed on large platforms. An important issue is how to ensure a high level of consumer protection for all digital content and services. At the same time, new rules need to take greater account of environmental protection issues.

Within the context of the DSA, it is necessary to review the current regulatory regime to ensure that it takes sufficient account of the threats to fundamental rights associated with digital services, in particular freedom of expression, the autonomy and decision-making sovereignty of the individual, as well as the protection of privacy, the right to non-discrimination and entrepreneurial freedom. This also brings into focus a number of new areas which are not or are only rudimentarily regulated in the e-Commerce Directive. This applies in particular to the platform economy in its various manifestations, which also includes the combating of criminal offences, punishable hate speech and disinformation in social media.

For these reasons, the country-of-origin principle and the cooperation mechanism of the e-Commerce Directive in its current form need to be re-examined, at least with regard to the regulatory regime on illegal content and criminal hate speech. It should also be ensured that the existing system of the CPC Regulation is not undermined.

1. Illegal goods and services

Platform operators should take stronger protective measures against the distribution of illegal goods and products not intended for trade, including live animals and plants, and illegal services.

2. Illegal content

The voluntary efforts of platforms are no longer sufficient to effectively prevent the distribution of illegal content. There is a need for binding rules, whereby non-compliance is subject to sanctions. It is also important for the platforms to have a reporting and redress system that is directly accessible and permanently available. Platforms should have to report on all measures.

3. Activities which may cause damage ("harmful") but are not illegal in themselves

New rules for the digital economy need to go beyond just regulating illegal goods and content. The dissemination of information and content that is not (yet) illegal can also be harmful in many ways, particularly disinformation and activities relevant to the protection of minors.

In order to combat disinformation, the Federal Government advocates that social networks should be encouraged to prioritise relevant, authentic and reliable information according to – if necessary – legally defined and officially/judicially verifiable standards, which take adequate account of freedom of opinion, and to do so using transparent processes. Demonstrably false information which could lead to serious risks for the individual or society should be subject to

lower priority, warnings or deletion. Users should be helped to find different points of view on an issue. A transparent complaints mechanism in both directions should be ensured, for which a common understanding of disinformation is necessary.

The Federal Government considers the voluntary commitments entered into under the Code of Practice on Disinformation (October 2018) to be an important but not sufficient step towards protecting users and societies from disinformation. It needs to be examined whether voluntary commitments need to be supplemented by a regulatory framework. The starting point should not be the content of the disinformation; instead, a framework should be established for the (technical) dissemination or selection of information and for checking the authenticity of user accounts, which should be monitored by means of far-reaching transparency obligations towards the public and professional circles and by introducing a supervisory mechanism.

The responsibility for complying with these obligations should lie with the operators of online platforms, regardless of where they are based (inside or outside the EU). The obligations could be staggered according to the size of the online platforms. Platforms should be required to ensure compliance with these obligations by setting up appropriate internal processes. In all measures, the protection of the fundamental right to freedom of expression and protection against harmful content need to be balanced in accordance with the relevant legislation and in a proportionate manner. These decisions must be taken by trained staff.

The supervisory structures in this specific area should in principle be independent and detached from the state and staffed with a diverse mixture of all relevant stakeholders; when it comes to compliance with general laws, a different regime can apply. It should be noted that the same regulations and supervisory structures applicable to content providers cannot simply be re-applied to the platforms. It should also be noted that content provided by broadcasters, for example, is already subject to extensive Europe-wide minimum standards for content under the AVMS Directive, compliance with which is ensured by the supervisory authorities of the broadcaster's country of origin. Press offerings are subject to the sole self-regulatory control of the Press Council. Monitoring procedures need to be established, as do possibilities for users to complain or take legal action.

Specific obligations should apply to the dissemination of political advertising or party-political content, and should also take account of new technological developments.

4. Clarification of obligations for online platforms and other digital services

The Federal Government welcomes the fact that the COM discusses a number of ambitious policy options in its combined roadmap / initial impact assessment (hereinafter: initial impact as-

sessment). In particular, the Federal Government advocates that the obligations of platform operators be clarified, harmonised and deepened and hence that regulations on responsibility, obligations and transparency for digital services (policy option 2) be introduced.

Such approaches should not be limited to specific sectors or business models, but should cover all those online services (i.e. social networks, messenger services, platforms, etc.) which are used by citizens very broadly and where they therefore depend on a higher level of protection through efforts or obligations entered into on the part of providers.

In the view of the Federal Government, online platforms should be obligated to provide procedures that enable users to report illegal activities in an easy manner, including via anonymous reporting channels, without any obligation to disclose personal data. As a minimum, complaint management should also include the review of such reporting within certain response times and the subsequent deletion/blocking of access to any illegal content and goods. In addition, the notification and decision should be communicated to the users involved, and the decision be reviewed upon request.

Consideration should be given to the use of varying degrees of stringency depending on the size of the service provider – although this is irrelevant for certain niche areas – and depending on the reach of the platform and the risk of illegal content being distributed (risk-based approach). The more distant the activity of the intermediary is from the content transmitted, the fewer requirements should be imposed on content-checking.

An EU legislative act could be adopted to establish a basic catalogue of content that is illegal across Europe and should be deleted or to which access should be blocked across Europe. At the same time, however, all Member States should have the possibility to define further content which is considered illegal in the respective Member State and is to be deleted or blocked in that Member State. While there is considerable agreement between the Member States on which statements are tolerable and which are punishable, there are also substantial differences. The criminal law assessments of the Member State in which the effects of a statement occur cannot be ignored, especially since the effects of any unhindered dissemination of unlawful content can have a direct impact on national democratic systems. When it comes to the deletion of illegal content, it will therefore be crucial to ensure that Member States have sufficient room for manoeuvre. The regulation of illegal content involves the balancing of the legal interests and fundamental rights of those affected by illegal content with the freedom of expression of the authors. It needs to be ensured that legal content is prevented from being deleted (over-blocking) and the diversity of opinion that is protected by fundamental rights must be preserved.

Platform operators' decisions to remove content that violates self-imposed community standards should not be arbitrary, but should be based on pre-established, transparent criteria which at

the same time do not provide for any control of journalistic and editorial content. The aim in setting up a new regulatory system is to find a balanced solution between the risk of arbitrary/uncontrolled influence by the platforms and that of unjustified influence by the state in what is a highly sensitive area in terms of freedom of expression. To this end, platform operators must also be required to ensure transparency on how their standards are applied when it comes to deleting/blocking users' content.

In addition, decisions of the providers on how content should be published (e.g. content ranking, timing, access restrictions for certain groups, as well as fact-checking notices) have a significant influence on the respective expression of opinion and democratic discourse. In order to preserve all of the fundamental rights positions affected, it is crucial that the powerful decisions of the platform operators are taken solely on the basis of narrowly defined and transparent criteria that respect the pluralism of opinion and after careful and targeted examination, and that there is scope for effective review, i.e. appeal procedures and judicial redress.

In order to assist with these checks, domestic contact persons can be appointed, e.g. authorised agents for legal proceedings. This will make it easier for citizens to bring disputes with “their” providers before independent courts. To protect the fundamental rights involved, various other safeguards can also be provided for within the respective regulatory framework. The personnel at a particular service provider who decide on the way in which content should be treated should be sufficiently qualified and receive regular training and support. The provider’s management staff should carry out regular checks on how complaints are handled and remedy organisational deficiencies straight away.

In addition, a procedure should be made available by which both the complainant and the author of the content can request a review of a decision taken. This can also include a facility whereby the provider is able to delegate its decision on how certain content should be treated to a ‘regulated self-regulatory body’ which ensures that reviewers have the necessary expertise and are independent.

With respect to the European legislative act, consideration should also be given to including provisions to facilitate criminal prosecution and civil enforcement against the author of the illegal content. This may include information rights of law enforcement authorities and persons concerned, reporting obligations to law enforcement and/or security authorities or, where appropriate in individual cases, obligations for providers to supply identification information.

In order to reach digital services and particularly sellers based outside the EU, it may also be necessary to introduce at European level special rules on the protection of intellectual property rights on product piracy.

The Federal Government welcomes the transparency and reporting mechanisms envisaged by the Commission for certain artificial intelligence (AI) systems used on platforms. In particular, small and medium-sized enterprises (SMEs) and start-ups must not be disproportionately burdened so as not to hamper innovation. While the ever-growing range of applications for AI systems can generate major economic, social and individual benefits, it can also entail risks, such as a lack of transparency in AI systems, the perpetuation of discriminatory structures or, in special cases, the opacity of neural networks ('black box effect').

Digital goods and services for consumers should be designed in a user-friendly way from the outset ('by design' and 'by default'). In this context, it should be legally binding for websites and digital services to be designed in a fair, appropriate and user-friendly way. This also includes stronger measures against misleading 'design tricks' and 'psychological tricks'.

There may be a public interest in the use of legislation to create or facilitate access to non-personal data and information, in particular where public interests are directly affected and there are insufficient market-based incentives to grant access to data. Legal measures can create incentives for online platforms to provide voluntary access to the data and information they hold. However, in certain circumstances, it may also be necessary to make access rights or obligations to provide access legally binding.

When examining potential legal measures, consideration will have to be given to what specific data sets ought to be covered by any legal right of access, and what the nature and scope of a legal right of access could look like in practice. Access to data and information on platforms for courts should be governed exclusively by the relevant national law on judicial procedure. The removal of content is a particularly sensitive area which not only affects individual rights, but also concerns the forming of public opinion, which is crucial to ensuring that democratic systems are able to function as a whole. The aim is also to counter the inherent dangers of over- or under-regulation. For this purpose, it seems useful for the scope of the reporting obligations to be oriented towards those under the German *Netzwerkdurchsetzungsgesetz* (Network Enforcement Act – NetzDG), which could be proportionately graduated for the identification and removal of illegal content. For example, the transparency reports should first contain general statements on the efforts made by service providers with respect to content removal. The reports should also contain at the very least the number of instances in which content has been removed, broken down by complainant (complaints body or user) and reason for complaint, as well as significant changes compared to previous reporting periods. The transparency reports should be sufficiently standardised in order to ensure that they are able to be compared.

In addition, particular attention should be paid to any automated preparation of decisions/decision-making as this carries a high potential risk. It is true that automated systems offer advantages in terms of providing increased work capacity and higher speed. Provided that they are sufficiently technically advanced and are programmed in accordance with democratic principles and the rule of law, they can enable accurate and fair decisions to be taken. However, the risks of automated systems lie in their lack of transparency for the general public and the impenetrability of the principles underlying their decisions. It should be made mandatory for information on data sets used for programming/training AI systems to be made available. Appropriate safeguards should be provided when it comes to the use of systems that are likely to undermine the protection of individual rights or the interests of civil society.

The reporting obligation should also include information on the nature, scope, and main principles underlying the functioning of any voluntary automated procedures used for the detection of content or goods to be removed. It should also include information on the training data used and on the mechanisms employed by service providers to verify said procedures. In order to make the decisions taken by the service provider easier to understand, the obligation to report also needs to include a description of the criteria for deciding whether certain content should be removed and of the verification process. Finally, the transparency report needs to be comprehensible and easy to find in order to enable the intended public control to be effective.

As is currently provided for under Article 17 of the e-Commerce Directive, consumers should be able to assert their rights under a contract with a business in an out-of-court procedure which is easily accessible and thus saves the costs and risks of going to court. It may also be necessary for there to be collective redress mechanisms in order to ensure a high level of consumer protection.

The Federal Government is also committed to ensuring that consumers can rely on strong and independent consumer organisations to provide advice and information and to support them in exercising their rights. This also includes existing European structures, such as the European Consumer Centres Network (ECC Net).

In the case that illegal content that has already been published, those responsible for platforms should react promptly and, if and when necessary, should communicate and cooperate with law enforcement authorities on the basis of applicable legislation.

A trained team should be available to cooperate with and respond to requests from law enforcement authorities in order to ensure that requests are dealt with and that content is deleted without delay. In the case of serious criminal offences, the identification of specific criminal content should be subject to a legal obligation for online platforms to notify law enforcement authorities.

5. Review of the liability regime for digital services

The Federal Government welcomes the fact that the Commission is now putting forward for discussion a review of the system of accountability for digital services and online platforms. This is because the ‘notice and take down’ principle, which currently exists as a result of the provisions of Articles 14 and 15 of the e-Commerce Directive, does not offer platforms any incentive to take measures against illegal activities in their own interest. Since the platforms set the framework and usually have a dominant influence on the platform activities of third parties, the Federal Government believes that the existing provisions should be changed into a duty of care or obligations to safeguard against sources of danger on the part of the platforms. However, a distinction must be made between the regular contractual liability of a platform on which goods are offered and the non-contractual liability of a platform on which illegal content is disseminated by users.

As is also envisaged in option 2 of the initial impact assessment, e-commerce platforms and online marketplaces should be legally obliged to take possible, reasonable and, where appropriate, automated due diligence measures to protect consumers (no blanket upload filters). To the extent that it is possible for them to do so at economically reasonable expense and effort, platforms should ensure that no prohibited or counterfeit products are advertised and no fake shops or other fraudulent offerings appear on the platform.

When establishing appropriate civil liability, the size of online platforms should be taken into account so that strengthening the liability of online platforms will not go on to constitute a barrier to market entry.

However, it should remain the case that the responsibilities of a seller and a platform should remain clearly delimited: the platform must not be held responsible for the quality of the goods advertised on it; this must remain the responsibility of the seller alone.

A further condition for the non-contractual liability of platforms vis-à-vis right holders is that Union law provides for platforms to bear civil liability for any dissemination of illegal content by their users. Non-contractual liability continues to remain within the competence of the Member States. This means that only the rules on accountability are able to be harmonised under Union law. When revising the Union's accountability rules, attention should therefore be paid to their consistency with national liability law and also with other reforms under consideration at EU level.

The review of the liability regime is also of considerable importance for criminal law. The European liability regime must not preclude the ability of Member States to criminally pursue plat-

forms set up to enable or to encourage the committing of criminal offences by third parties, including in cases where operators are only aware of the criminal intent, but have no positive knowledge of any specific criminal transactions.

In the view of the Federal Government, the concept of the intermediary in the e-Commerce Directive is no longer appropriate. ‘Intermediaries’ in the form of online platforms have since taken on a central role as they control information flows, making them more than mere intermediaries of only a “mere technical, automatic and passive nature”. In addition to the category of the passive host, there is an increasing number of providers who do not remain completely passive but who do not meet the definition of content provider. These platforms which, in addition to hosting, also influence the presentation of content or deliberately commercialise the content of their users without posting it themselves, should be distinguished from passive hosts and the liability privileges linked to this definition. Thus, separate rules for those services could be considered.

In view of the diversity of functions assumed by large platforms, subsuming the various types under the categories of services should not be undertaken across the board for the entire platform, but rather for the individual parts of a service. Whether and which obligations apply to or are appropriate for the various parts of a service must be assessed in particular in relation to the importance of the part of the service concerned for the overall service. Article 28b(3) of the amended AVMSD could serve as a blueprint for this. Sector-specific EU legislation (AVMSD, DSM Directive) should be maintained in the new legislative package, but it should be made clear how the directives relate to each other. Synergies with sector-specific legislation should be used. The definitions contained therein can be built upon to avoid further fragmentation of the law. The same applies to well established supervisory and control structures. In particular, the definition of video sharing platforms set out in Article 1(1)(aa) of the amended AVMSD must be taken into account. If partial regulation of content is also sought, the aim must always be to achieve only the minimum level of harmonisation necessary, as high national standards should not be undermined. In addition, the protection of freedom of the press and freedom of opinion in particular must be ensured. Furthermore, provisions determining the terms of independent supervision set out in sector-specific legislation (such as Article 30 of the amended AVMSD) must not be undermined by horizontal rules.

The information obligations of platforms and the sanctions available for breach of Article 5 of the e-Commerce Directive should be examined or clarified, as many illegally operating online platforms, in particular websites that structurally infringe copyright, deliberately accept that they breach this article by concealing their identity or that of their business customers. The identity of commercial users of platforms, including advertisers, should be established by the platforms by means of reliable proof of identity (“know your business customer”) prior to inclusion on the platform. It should also be possible to establish the identity of the platform operator beyond doubt.

6. Country-of-origin principle

a. Principle under the e-Commerce Directive

The country-of-origin principle was introduced by the e-Commerce Directive in order to make it easier for the then young and mostly small companies to provide cross-border services and to facilitate rapid growth. This European approach of using the country-of-origin principle particularly reflects the freedom to provide services. It is also the core of European media regulation under the AVMSD and an important component of how European media are regulated.

b. Current situation in the field of criminal hate speech

However, this approach can only produce balanced results if there are sufficiently harmonised rules across Europe and if the authorities of the respective home country have sufficient capacity to act in order to be able to monitor “their” providers throughout the whole of the internal market. This is increasingly difficult to ensure in cases where very large and powerful companies have since established themselves in the market without the relevant general standards of protection having been (able to be) raised and, more importantly, enforced in each Member State.

The area of illegal content, criminal hate speech and disinformation, in particular, which has emerged in recent years, poses very special challenges: the growing volume of reported content related to a wide range of criminal activities may already exceed the capacities of a single national authority to respond. Moreover, it will often be the case that the objectionable content is presented in languages other than the language of the country where the authority is based, and that users who contact the authority speak a different language. Following the approach that all Member States should have the possibility to define, in addition to a European basic catalogue, further content which, in accordance with the freedom of expression guaranteed in the Charter of Fundamental Rights in the EU (CFR), is considered illegal in the respective Member State and must be deleted or blocked in that Member State, the authority in the home country will frequently be faced with the problem that such criminal content can often only be understood and evaluated within the national context. The staff of the authority in the home country will usually not know the conditions under which specific content is considered illegal in other Member States and must therefore be deleted or blocked.

While the current e-Commerce Directive allows exceptions to the country-of-origin principle, these do not meet the current challenges in the area of criminal hate speech. The procedures to be followed under Article 3(4) of the e-Commerce Directive are sometimes cumbersome and lengthy, resulting in a lack of legal certainty.

In the view of the Federal Government, however, it must be ensured that illegal content can also be dealt with promptly and effectively in a cross-border context. Member States should not be put in a position where they have to accept the dissemination of illegal content on their territory.

In clearly defined exceptional cases, Member States should be able to take action against punishable content on their own territory if the provider is based in another Member State. Consideration should also be given to the possibility of granting specific exceptions to the country-of-origin principle in certain other areas.

c. Media

With regard to the regulation of media content (in particular broadcasting and the press), the independence and freedom from state control / state interference of the regulatory authorities and voluntary self-regulatory bodies must be maintained. It is not advisable to have a state and centrally controlled EU regulatory authority in the media sector (in particular broadcasting and the press). The existing regulatory authorities in the audiovisual sector must be adequately equipped for cross-border enforcement. Cross-border cooperation should also be improved and streamlined.

7. Online advertising

As the exchange of information and thus the creation of value is increasingly shifting to the internet, the issues of online advertising and competition in the digital sector are gaining considerable importance.

Advertising revenues are a source of financing for many platforms. Such platforms therefore seek to keep users on their sites as long as possible and entice them to make as many “clicks” and engage in as many interactions as possible. This encourages the display of increasingly dramatic content. As a result, this can lead to fake news, conspiracy theories and incitement to hatred, as such content has a particularly high interaction rate.

It should be examined whether users should be given the freedom of choice to use online intermediary platforms but without personalised advertising and whether, in the case of personalised advertising, the criteria for the basis on which the personalised advertising is displayed should be specified.

Economic, political and ideological advertising measures should be kept in an archive to create transparency. Information regarding the name of the client, target group, number of placements and costs should also be documented. Each person concerned should also be able to understand why a particular advertisement is being displayed to them. Every person concerned should be able to change their advertising profile. It should be examined whether further transparency obligations are necessary or whether existing transparency obligations can be made more tangible.

The all-encompassing data collection and the considerable asymmetry of information increasingly enable companies to personalise prices and products through data analysis according to

the information they hold on customers. For example, it is possible for an algorithm to set different prices depending on the individual customer's willingness to pay. This can be accompanied by distributional effects which both increase welfare and – at least for certain groups – can lead to price increases. In principle, it could be envisaged for certain groups to be excluded from particular services. These developments should be monitored. Regulatory action should be taken if this is necessary to ensure participation or fair distribution.

B. Regulation of platforms with a gatekeeper function

The Federal Government shares the view of the Commission that large platforms are able to control increasingly important platform ecosystems in the digital economy. This creates the danger that fair competitive opportunities, in particular for innovators, creative people and new market entrants, are not sufficiently ensured in markets that are characterised by platforms with significant network effects.

This also raises particular challenges for consumer protection. The reason for this is that gatekeeper platforms have strong market positions as intermediaries, especially between suppliers and consumers, and have a considerable influence on supply, demand, freedom of choice, contractual conditions and prices. The new legal framework for gatekeeper platforms should therefore not only focus on fair competitive conditions, but also on protecting the rights of consumers. When it comes to gatekeeper platforms, it is also an important aspect for consumers that freedom of choice is preserved as a fundamental principle of consumer protection, as this also helps to prevent lock-in effects.

The limitations of existing competition law are, firstly, that it requires lengthy procedures due to the high standard of proof with respect to infringements, secondly, that it sets high standards of proof with respect to the dominance threshold and provides few possibilities for taking action below this threshold, and thirdly that it does not provide sufficient scope for (clear) interpretation of Article 102 of the Treaty on the Functioning of the EU (TFEU), particularly with regard to leveraging market power into other markets.

The Federal Government also shares the Commission's assessment that the current European legal framework (including competition law) does not sufficiently ensure fair competitive opportunities for all market participants in markets that are characterised by large platforms with significant network effects acting as "gatekeepers". These platforms should therefore be subject to 'ex-ante regulation'. It should also be examined whether such ex-ante regulation should also apply to platforms which do not yet perform a gatekeeper function but have significant intermediary power.

In order to strengthen innovation, competition and access opportunities in the platform economy in particular, the Federal Government has long been of the opinion that enforcement instruments must also be strengthened vis-à-vis digital platforms with a strong market position.

With regard to the ‘ex ante’ instrument proposed by the Commission, the Federal Government favours a combination of options 3a and 3b, i.e. the introduction of codes of conduct and bans on certain practices (‘blacklisted practices’) for certain online platform companies (option 3a), as contained in the initial impact assessment, and the imposition of more far-reaching remedies by the competent authority in individual cases (option 3b). Both regulatory approaches under option 3 should avoid substantive interference with primary competition law by means of a clear definition of the scope of application. Dominant platforms should continue to be addressed by the competition authorities. Regulatory rules of conduct should apply to gatekeeper platforms and, where appropriate, to platforms with significant intermediary power, without requiring a comprehensive market analysis in each individual case.

With regard to the addressee status, the Federal Government supports an approach that ensures the purpose of the rules, i.e. protection against the exploitation of a gatekeeper function, combined with a sufficiently rapid identification of the factors determining the addressees.

Seeking to ensure clear responsibilities and to avoid inefficiencies with regard to competition law and the New Competition Tool (NCT) in particular, the Federal Government is in favour of the Commission being mainly responsible for enforcing the ‘ex-ante instrument’ at European level in pan-European cases. Options 3a and 3b, which provide for the possibility of analysis on a case-by-case basis, may lead to interferences primarily with Article 102 TFEU, which is to be complied with as primary law, with regard to determining addressee status, a potential balancing of interests and the development of remedies. For this reason, it also makes sense that in this matter of European scope such an instrument is placed with the Commission.

When it comes to the area of the protection of cultural identity and diversity, there are strong national interests at stake. The regulatory competence for cultural diversity, media and ensuring diversity is in principle the responsibility of the Member States (principle of subsidiarity) and must not be undermined by EU legislation. It is therefore necessary that the legislative acts of the DSA Package provide for sufficient powers of derogation or exemptions for certain sectors within the Member States. Against this background, any potential abusive practices must be identified at an early stage. Many potentially abusive practices of digital platforms are already known from practical experience, but they can take different forms depending on the context:

- Self-preference in the case of vertically integrated platform operators: favouring of proprietary products and/or services, e.g. through discriminatory rankings or pre-installation/default settings in favour of proprietary offers.
- Preference for specific third-party suppliers, e.g. through discriminatory rankings or pre-installation/default settings in favour of third-party goods or services.
- Refusal of access to the digital platform (permanent or temporary) or to other essential functions.
- Unfair terms and conditions: imposition of exclusionary commercial terms and conditions which only allow access to the digital platform under certain conditions, for example by means of blocking certain functions or setting unreasonable performance targets. Imposition of terms and conditions which are unfair to commercial users and end users, for example for access to the digital platform, to data without personal reference or to other core functionalities.
- Restrictions on access to data which platform users cannot generate or collect themselves or which can only be generated or collected with disproportionate effort.
- Lack of transparency with regard to the strategic use of unclear or incomplete business conditions as well as the comprehensibility of the functioning of algorithms (e.g. ranking).
- Tying and bundling requirements for platform users.
- Communication restrictions imposed on commercial users to provide information about the platform to their own end users.
- Interoperability constraints, such as the refusal to allow the integration of alternative payment methods in certain applications without objective justification for the refusal (e.g. security or data protection concerns).

When developing future codes of conduct for relevant digital platforms, distinct and sometimes conflicting aspects need to be considered and reconciled. Rapid intervention at an early stage is crucial whilst ensuring legal certainty for all parties involved. It is further necessary to establish an appropriate level of regulation and to strike an appropriate balance between directly applicable obligations and conditions under which action is to be taken by competent authorities in individual cases.

1. Regulatory approach

In addition to globally operating platforms, (specialised) digital platforms can also create serious problems for certain customers, causing lasting damage to competition. For this reason, the future regulatory framework should also provide for the possibility of adopting individual remedies. It should however be taken into consideration that, in addition to the complementary rules of the NCT currently under discussion, existing competition law already allows for individual remedies to be taken in the event of abuse of a dominant position in individual cases.

2. Addressees

With regard to determination of the addressees, an approach should be adopted which combines the purpose of the rules, i.e. the protection against market power, with a sufficiently rapid identification of the factors determining the addressees. In the view of the Federal Government,

the group of addressees should include major gatekeepers. It should also be examined whether platforms which do not yet perform a gatekeeper function but have significant intermediary power should also be subject to the regulation.

Companies can be qualified as platforms with a gatekeeper role based on factors such as high user numbers and turnover, significant data power through access to competitive information, limited switching possibilities, lack of multi-homing and the (de facto) obligation of users to accept the terms and conditions imposed in order to be able to reach other user groups. It is important that the group of addressees can be directly identified based on clearly defined absolute thresholds for certain business areas, especially for potential addressees of legislation ("a set of clear criteria"). In addition, it should be possible to identify a digital platform as an addressee of mandatory rules of conduct in individual cases. As regards digital platforms based outside the EU, the impact of their activities within the European internal market should serve as the point of reference. In addition, directly applicable, general rules of conduct should set objective and easily verifiable absolute thresholds above which a digital platform with a gatekeeper function can be assumed to be an addressee. The following structural and specific features (not exhaustive and not cumulative) could be taken into account in case-by-case analyses in order to identify platforms with significant intermediary power and, in particular cases, with a gatekeeper function:

- Strong direct and indirect network effects,
- Considerable availability of data from users and all providers as well as competition-relevant data from the specific business area,
- Significant economies of scale and scope,
- Significant barriers to starting and expanding business in technical and/or legal terms,
- Lock-in effects (high switching costs),
- Gatekeeper function vis-à-vis users and/or role as indispensable business partner for commercial users (including competitors and suppliers of complementary goods and/or services),
- Significant financial resources and/or easy or privileged access to capital markets, and
- Part of an ecosystem.

Provided that the absolute limits are not exceeded, for example in the case of specialised digital platforms, there should be the optional possibility to identify that a digital platform has a gatekeeper function or significant intermediary power in individual cases, for example by taking into account the features listed above. For this purpose, the competent authority should be able to officially determine, by way of notice, the addressee status of a digital platform for a certain period of time. It should be able do this either ex officio or on the basis of a complaint within its discretion by carrying out an examination on a case-by-case basis.

If such criteria are to be used to determine market power, numerous aspects and complex issues need to be taken into consideration. In German law, for example, such factors arise from Sections 18(3) and (3a) of the *Gesetz gegen Wettbewerbsbeschränkungen* (Act against Restraints of Competition – GWB).

3. Rules of conduct

For the above reasons, the Federal Government would prefer directly applicable general rules of conduct for the digital platforms covered, combined with the possibility of individual remedies being imposed by the competent authority. As a general rule of conduct, it should be established that the platform must behave in a neutral manner and must not favour itself. For example, general non-discrimination rules could be laid down in the rules of conduct and be covered by a prohibition. The introduction of a requirement for large platforms to be interoperable vis-à-vis other smaller platforms could strengthen users' rights to data portability and counter lock-in effects. For example, transparency rules exceeding the requirements set forth in the P2B Regulation could be defined as mandatory. If a digital platform infringes these directly applicable rules of conduct, the competent authority should be able to impose sanctions and enforcement measures ex officio or following a complaint by exercising its discretion.

4. Additional comments on option 1 (extension of the P2B Regulation)

In view of the overriding practical importance of the model of online platforms and their considerable relevance for the everyday life of consumers, a comprehensive P2C Regulation should be considered that could be designed similar to the P2B Regulation, which applies to companies. Such a regulation could be used to establish high consumer protection standards and to consolidate and strengthen the rudimentary rules hitherto contained in other directives on consumer contract law, and to specifically design them for platforms. In addition, certain business practices towards consumers should be prohibited and fair and appropriate ranking and evaluation systems should be considered in the context of obligations for platforms. Similarly, each digital service should be required to designate a representative in the EU as a contact point for users. This strengthens the confidence of EU users in European providers and creates a level playing field for all providers in the EU, thereby benefitting the EU platforms themselves.

5. Remedies

In addition, the competent authority should be empowered, ex officio or on the basis of a complaint within its discretion, to impose individual and proportionate remedies exceeding these general rules of conduct on the basis of a case-by-case analysis, in order to address specific difficulties relating to specific digital platforms. In this context, some of the transparency obligations under the P2B Regulation could also be further developed to prohibit specific conduct (e.g.

Articles 6, 7 and 10). In addition, it could be envisaged as a last resort to prohibit a vertically integrated platform from operating itself on the market in which it is acting as an intermediary. If these remedies are not implemented by the digital platform within the prescribed time frame, the competent authority should be able to impose sanctions and enforcement measures, including fines.