BUSINESSEUROPE

POSITION PAPER

14 June 2017

The proposal for an ePrivacy Regulation

KEY MESSAGES

1. This proposal should fully align with the General Data Protection Regulation and not disrupt the current balance between protecting personal data and facilitating innovative business models.

2. More clarity is needed to determine the relationship between this proposal and the General Data Protection Regulation so that stakeholders understand which rules apply in instances where both are possible.

3. More clarity is needed to determine the scope of this proposal and which stakeholders are covered by it. A level playing field should be found between those stakeholders offering the same service.

4. The full range of permitted processing capabilities afforded by Article 6 of the General Data Protection Regulation should also apply to this area of electronic communications.

5. Machine to machine communication processes that have no clear or recognisable data subject should be removed from the scope of the proposal.

6. Quality should take priority over speed. Sufficient time is needed by the co-legislators to fully consider and improve the proposal, stakeholders who will apply the final result should also receive sufficient time to prepare to implement the final Regulation

WHAT DOES BUSINESSEUROPE AIM FOR?

An update to the framework in the area of electronic communications that will actually enhance trust and confidentiality in a proportionate, legally certain, robust, technology-neutral manner while not duplicating or contradicting the General Data Protection Regulation.

Context

Electronic communications providers are a vital part of European Industry and are the backbone of the Digital Single Market. Not only do they answer the exponential connectivity needs of businesses and citizens', but they provide the base to which Europe's digital economy has been built upon. Through investment and maintenance of their networks, these providers enable Europe's digital capabilities.

Online service providers (OSPs) are another important addition to Europe's flourishing digital economy. Often taking advantage of innovative communication methods, eg. social media, content, internet or cloud based services – even from adjacent industries, OSPs benefit consumer choice, to enable new business models to be formed. This is highly relevant for Europe's start-ups and small medium enterprises (SMEs).

This evolution of electronic communications services is having an even wider impact on other industries. Businesses depend on the efficiency of their communications, most operating in Europe will use some form of electronic communication provider and service in their daily operations, eg. the manufacturing industry using real time inventory technology to inform customers of available stock. Advantages are also being taken in the business to consumer context, eg. the hospitality industry using automated booking systems.

Enabling reliable connectivity and more innovative services is clearly beneficial for Europe's economy, the internet economy alone contributes some 700 billion EUR a year or 5% of GDP. The societal benefits are also significant, high speed connectivity is a prerequisite for innovative public services, it also means more efficient agriculture, greater use of energy distribution, smarter transportation and health. European industry is also increasingly dependent and supported by sensors connecting different devices and machines to improve efficiency and leveraging industrial processes.

These opportunities have caused a natural explosion of electronic communications data in terms of the sheer amount of content, devices and variety of actors involved. Around 80% of Europeans have a mobile phone and 315 million European's use the internet every day. As these communications cover personal and non-personal data, consideration should be given to the most appropriate legal framework.

The existing ePrivacy Directive reinforces trust and confidentiality of electronic communications while the soon to be implemented General Data Protection Regulation (GDPR) should eliminate privacy concerns. Further to this, the ongoing revision of the European Electronic Communications Code (EECC) provides the basis for many definitions this proposal relies upon.

It is important that this framework remains balanced. In the interest of innovation, legislation is not needed for every technological step forward. In fact, policy makers should only legislate in response to existing failures in the market. Championing better regulation in this manner will ensure the full economic and societal benefits that electronic communications providers, OSPs and their users afford.

A balance needs to be found between the right to respect private and family life, including the confidentiality of communications, with business opportunities and consumer trust. Technological innovation should be understood and fostered instead of being held back by stringent rules. It will always remain ahead of actions undertaken by policy makers.

The co-legislators to provide sufficient time to implement the final Regulation. Businesses are already preparing to apply the GDPR. It is therefore crucial to grant them sufficient time to properly understand and prepare to apply the additional rules of this proposal. It is currently uncertain what the outcome of discussions will be and as a result businesses are unsure whether they have to simultaneously prepare to comply with this proposal as well.

We understand the Commission's intention is to speedily wrap up of this proposal through the co-legislative process by May 2018 to coincide with the application of the GDPR. While this ambitious timeframe would be commendable for a proposal that complements instead of redefines the GDPR, we do not believe that it has been achieved in its present form. **The co-legislators need a greater amount of time to fully understand and evaluate the impact of the current proposal.**

While it is also unlikely that negotiations will be concluded to enable this Regulation to come into force on the same date as GDPR. **The Commission should set a realistic timeframe for adoption and application.** Particularly to give businesses greater certainty.

BusinessEurope outlines its position on the Commission proposal below and offers suggestions on how it believes both co-legislators should heavily amend its provisions to ensure a proportionate and legally certain proposal for electronic communications providers, OSPs and their users.

1. Scope

BusinessEurope agrees that the electronic communications landscape has changed since the coming into force of the Directive on Privacy and Electronic Communications (2002/58/EC). It is therefore understandable that those OSPs are brought in line with traditional telecommunications providers that often process the same data and offer electronic communication services as a primary part of their business model. In fact, OSPs already prioritise the privacy of end-users' communications. A level playing field is beneficial for competition of all businesses offering the same services. Whether they are the same should be assessed and its outcome should not hinder innovation or the benefits offered to consumers.

However, this proposal will not enable a level playing field for businesses in the area of electronic communications. Instead Recital (11) includes *"communications services that are ancillary to another service"*. While confidentiality is a prerequisite for all service providers in this area, including services ancillary to another within the scope of this proposal will adversely impact wider categories of services that only use some form of communication as a secondary function. Indeed, the Article 29 Working Party already argues that *"the definition of 'electronic communication service' does not mean that service providers who offer both electronic communication services and content services are outside the scope of the provision of the ePrivacy Regulation".* Therefore, this proposal can impact any online service, bringing most service providers into its scope.

This will not achieve a level playing field. It will only lead to greater burdens being placed on services that do not offer electronic communications as a primary part of their business model, but as a component to enable their primary service to function. This will adversely impact a great number of applications and services from event schedulers to online gaming and photo editors to mobile banking.

Machine-to-machine (M2M) communication is also included within the scope of the proposal through the definitions of 'electronic communications service' used in Article 4(1)(b) and as described in Recital (12). This means that the processing and storing of electronic communication content and metadata between machines is covered as well. This would introduce significant friction into a system whereby different entities electronically interact throughout business to business supply chains.

In practice, this will have a negative impact on significant new technologies for Europe's digital economy, such as Internet of Things technologies (IoT). It could also put the Industry 4.0 concept in jeopardy. The infrastructure that would be required to ensure automated consent is legally valid between machines would be enormous and in other instances impractical.

The territorial scope also outlined in Article 3(1)(b) and (c) in relation to services and terminal equipment is also practically problematic. It would imply that any device using a service from anywhere in the world while located in the EU has to reach the requirements of this proposal. Some devices and services may not have been placed on the market with the intention of offer to the EU, however they would still confusingly fall under this proposal.

Recital (11) and all references to communications as an ancillary service should be deleted from the proposal. This would not only achieve the Commissions' objective of building upon the EU Telecoms and data protection framework (which excludes these services), but would also better ensure the digital single market, industry and employment to take full advantage of digitalisation (as part of the Commission's Digital Single Market Strategy). This approach would also support the Commission's overall political guidelines of not frustrating innovation and competitiveness of SMEs, particularly in relation to Europe's applications community. Further to this, the GDPR already applies to these services, duplication is not required and could actually cause legal uncertainty in practice.

Recital (12) and all references to M2M communications should be deleted from the proposal. The scope should be narrowed to expressly exclude industrial and non-end user applications (B2B). When M2M communication is used it often does not involve personal data (eg. smart industrial farming or smart factories). The non-personal data that would also be subjected to this Regulation through M2M communication is excessive and will discourage digitalisation of industry (going against the Commission's Digitalisation of Industry Strategy). If data within these processes was personal it would already be covered under the GDPR, all the more reason to not create further legal uncertainty through overlapping legislation.

Article 3(1)(b) and (c) should include a reference to placing on the market. Otherwise a wide range of products and services will fall under this proposal even when not intended to. This would better align with the GDPR that is clear: mere accessibility of a service should not trigger the applicability of law. For example, tourists using devices and services when travelling to the EU that were placed on the market outside of it should clearly not be covered.

2. Permitted processing

BusinessEurope supports the fundamental right of confidentiality in communications. Businesses already ensure that only those parties involved in the exchange of a communication see it. For that communication to take place, technical steps to process the data are required. The draft ePrivacy Regulation generally treats any processing of

communications data, for purposes other than the basic act of facilitating the transmission of a communication, as an extraordinary action that is only permitted in narrow and restricted circumstances, eg. when a person provides consent. This approach may have made sense in an era when communication services had limited functionalities and people had few choices about the services they used, but it does not make sense today. Today, people often choose a communication service because of its "smart" features, which are increasingly powered by artificial intelligence. These features, like the automatic creation of calendar events, the display of "preview" content for shared links or the automation of tasks like helping friends meet up, rely on the processing of communications data.

We take note that the Commission suggests to regulate the processing of communication data, instead of the current approach in the ePrivacy Directive which ensures the confidentiality of communications. The Article 29 Working Party suggests that communication data generally is personal data, so businesses could apply Article 6 of the GDPR in relation to when that processing is lawful. This recognises several legal bases for processing personal data, such as: upon consent, in order to perform a contract, to fulfil a legal obligation, to protect vital interests, to carry out a public interest or a legitimate interest. However, the ePrivacy proposal will contradict the GDPR in this area and will dictate consent as the only method businesses can use to process data that is communicated electronically.

Article 6 of the ePrivacy proposal would prohibit any processing or interference with communications data without consent, with narrow exceptions that could realistically be used in only a limited number of circumstances, for example for security (Art. 6(1) (b) where it is *"necessary to maintain or restore the security of electronic communications networks and services"*. This closed list is not robust and will not provide the flexibility required to deal with future technical developments.

Further to this, the type of consent that is required to process content data goes far beyond that of the GDPR. It applies additional safeguards than the GDPR: proof that anonymisation was tried and does not work, a data protection impact assessment and prior consultation with a Data Protection Authority (DPA). Article 9(3) will further require that users are also reminded of their consent *"at periodic intervals of 6 months".* This two times a year check is burdensome and stricter then the GDPR. Forcing users to reconfirm their consent every 6 months will be burdensome on businesses and cause consumers to ignore information about how their data is used in practice, not to mention the added frustration to the experience of the service. In practice a single consumer uses a variety of apps and services and this will continue to grow.

Article 6(2) also extends the consent regime to metadata. Extending consent to metadata is impractical for multifaceted services – would consent need to be asked separately? Further to this, how can consent be collected from all parties included in automated communications?

These are just some of the reasons why we consider the type of consent required goes beyond that of the GDPR and can be viewed as *"consent+".*

The regulation changes the language used in the ePrivacy Directive on confidentiality through Article 5, not only does it restrict interception and surveillance, but also any "processing" of electronic communications data more broadly. Restricting the approach to confidentiality requirements to process data in the context of a *consent+* only regime goes beyond the intended aims of Article 5 and does not take the state and process of technology in practice into account.

The legal grounds provided by Article 6 of the GDPR should be replicated into Article 6 of this proposal. It is nonsensical as to why lawfulness of processing cannot be demonstrated by using the same possibilities as those included in Article 6 of the GDPR. Particularly as the Commission's intention is to align this proposal with the GDPR. Also, other processing methods such as "legitimate interest" offer high forms of protection. It should be understood that "consent" can be given carelessly or even bought by offering a "prize" in return for sharing data. Whereas "legitimate interest" requires a balance to be actively found between the fundamental rights of the data subject and the use of the data. This is consciously decided by the data controller and can be challenged by authorities. In practice, if "legitimate interest" does not work (the rights of the subject prevail above the business interests), consent is often used as a last resort. Dictating *consent+* will not simplify this policy area but instead create a separate track or privacy law for electronic communications that is more stringent than the GDPR. Not to mention the legal uncertainty surrounding *consent+* within this proposal due to the Commission's intention of applying it at the same time as the GDPR. It would be better to take the opportunity to learn from how consent is applied in practice through the GDPR before overriding it through this proposal.

Article 6(2)(a) and (c) should be deleted and all other references to metadata. We challenge the Commission's conclusion that states all metadata are high risk particularly when it is not considered personal data under the GDPR. In contradiction to its original objectives, this proposal will not lead to greater opportunities for businesses to process metadata. The proposal will mean metadata can only be processed based on consent, except in limited circumstances under Article 6(2)(a) and (b). Further to this, Article 6(2) only refers to electronic communications service providers and not network providers, although both service and network providers need to process data to detect technical faults or calculate incorrect payments. Processing of data for these reasons in practice is needed to improve services and overall user experience.

Article 6(4) of the GDPR should be replicated in Article 6 of this proposal to enable **"**further compatible processing" criteria as a lawful method of permitted processing. The connection between processing activities, its impact, the use of strong safeguards like pseudonymisation, the reasonable expectations of individuals and the inclusion of opt-out procedures, should be considered factors to weigh-up to allow further compatible processing based on initial permitted processing (eg. legitimate interest, performance of contract or compliance with an obligation). Aligning with the GDPR, this processing would be analysed through a privacy impact assessment and observed by supervisory authorities. This is already mentioned in Recital 17 of this proposal.

The word "only" should be removed from Article 6(3) to improve the legal certainty of the proposal. Otherwise, Article 6(3) seems to be in direct contradiction of Article 6(1). We also believe that the words "all end-users concerned" should be replaced with "end-users" in Article 6(3)(b). It would be impossible for a business to obtain consent from someone they do not have relations with.

The word "security" needs to be redefined to clearly cover both technical security and cyber security issues. The "availability" of networks also need to be included in Article 6(1). Third party devices connected to a network that make it available through processing data should also be enabled (eg. a router). This should also include devices of users.

Article 9(3) is not necessary and should be deleted. The right to withdraw consent at any time is already possible within Article 7(3) of the GDPR and should also apply in

the context of this proposal. Therefore, the introduction of an additional obligation to inform end-users at periodic intervals of 6 months of their right to withdraw consent is not justified. Co-legislators already deemed this unnecessary during the discussions over the GDPR as it was agreed such additional obligations would impose additional administrative burdens while not granting added value to the end-user. The same reasoning should prevail here. Reminding users of their consent every 6 months is unnecessary and will not achieve the objectives of the Commission to enable greater transparency of consumers. In practice, a proliferated *consent+* regime would frustrate users leading to further oversight of how their data is being used.

3. Storage and erasure

BusinessEurope understands the interest consumers have concerning the storage of their content and who can view it when using certain services. Businesses supplying these services are interested in the workings of their technology and user experience. While certain services dependant on storing users' data like cloud, webmail or music streaming, require content in order to function and deliver the conditions consumers expect, businesses use that content to make the service work and develop new products and services. Throughout this process, intelligible transparent information is given to the consumer on how their data will be stored. The consumer always has the ability to control and delete content upon request.

This proposal will restrict services dependant on users storing data. Article 7 requires the processing and storage of data to be anonymised or deleted after receipt of the message. This will limit and restrict current and future personalised based services that will no longer be able to rely on communications data once it is anonymised. Further to this, it would also mean that content data is erased upon receipt. This would render similar services to those listed above useless to consumers who actually expect their data, such as photos, emails and songs, to be kept for them to access again once communicated electronically. The erasure requirement would also prevent the abilities of innovative businesses from developing new services for consumers from the use of previously collected content and metadata.

Article 7 should be deleted. The services of various providers rely upon the ability to store content. It would be impossible to continue to offer these in practice otherwise. Further to this, the GDPR provides strong rights to the users, including the right to erasure and objection and therefore will continue to offer its high standard of protection. Article 5 of the GDPR which relates to processing of personal data will also apply to electronic communications. There is no practical reason to go against the Commission's intention of aligning with the GDPR. Article 7 contradicts this aim and stipulates anonymization and deletion of electronic communications data upon receipt.

Article 7(1) is also unclear on which rights of the GDPR need to be applied in practice when recording, storing or processing data. For example, will the right of data portability apply as an obligation to electronic communications data (metadata and content)? **If Article 7 cannot be deleted as proposed above, further clarity is needed on which obligations of the GDPR will apply in relation to storage.** We do not believe the data portability right within Article 20 of the GDPR should apply to electronic communications metadata. Not only is it difficult to determine the real need of this for end-users, but it would be difficult to implement technical solutions to allow for portability of such data. This also poses serious security and privacy risks for end users as the controller cannot guarantee privacy and security of such data once it is transferred to and stored by the subject.

4. Terminal equipment

BusinessEurope agrees that the confidentiality of the device used in relation to an electronic communication is just as important as the data within that communication itself. Devices deserve a shield of protection otherwise they would be open to misuse of user data. Businesses already ensure that this protection is afforded by such devices as: PCs, tablets, smartphones and any other smart device connecting to the internet. Without holistic protection, not only would users not buy these products but entire networks they operate on would be put in jeopardy. As a result, there is a vested interest to adequately protect devices by all bona fide businesses.

Access to the device is required to ensure it is protected. In practice, this takes place through updates that are offered or sometimes required on the basis of data access. Certain updates are optional on the basis of user consent that gives an element of control. Yet others are too high risk for that option. Usually due to the existential threat placed on the network an update to a device is made in order to protect it. In practice, this cannot take place only through user consent.

Article 8 requires consent as the predominant method to protect terminal equipment. This will place danger on various networks if a user does not keep up with requests for updates. Devices can be hijacked by hackers to send invalid communications to other users spreading breaches stealthily and quickly. Further to this, hackers could even access and damage networks alone through not granting their own consent to updates. Also, under the GDPR, consent is not considered to be given freely in the employer/employee relationship because of a possible hierarchy. How would employers push their employees to protect devices used in the work place such as their mobile phones? Dictating consent as the main lawful processing method in this manner will enable hackers to carry out more intricate cyberattacks.

Article 8 would significantly impact the functioning of the digital economy. Online advertisers support the digital economy through processing information about websites or apps that a consumer uses. This is essential for measuring the impact of the adverts used in association with them. Article 8 would limit this practice. Although it contains an exception for “audience measurement”, it would only apply where a business conducts the measurement itself. This renders measurement unlawful for most businesses as it is only larger online businesses that are capable of performing measurements without the need for third-party service providers. The exception also excludes measurement of advertising from its scope. This is an essential activity for website and app developers in order to appropriately charge advertisers for showing their ads, among other things.

Article 8 is also so broad that non-personal and M2M data is covered. This is a concern to smart industrial processes. Will robotics and sensors collecting data to ensure their maintenance have to grant consent each time a request is made? Not only will this be impractical in terms of efficiency but technologically infeasible. Factories of the future should become more effective and efficient not less. We cannot understand why non-personal industrial generated data, often processed between machines alone, would have to function in such a strict regulatory environment.

This will also directly impact citizens that are being enabled to use interactive devices (robots, multimedia monitors) that are connected to central systems (wifi, bluetooth) to answer their questions or give interactive displays. This could include providing a location of a shop in a commercial area or the best route to get to a bus stop. Making these services useful requires processing and storage capabilities of terminal equipment. This is carried out through lawful agreements between, for example, the

entity owning the equipment and the entity providing the service. In these contexts, how can *end-user's* give their consent when they have no relationship with the terminal? What is the law trying to protect?

The lawfulness of processing possibilities in Article 6 of the GDPR should be replicated into Article 8 of this proposal. The GDPR's approach reflects a balancing of the need to protect the rights of the data subject while also ensuring businesses can continue to provide digital services. Stipulating consent as the predominant method of lawful processing will not achieve the Commission's objective to further protect these devices. In fact, dictating consent in this area will hand hackers an easier route to access users devices while making it more difficult for businesses to protect their devices on behalf of their users. This will greatly impact the design of Internet of Things technologies just as they begin to proliferate.

3rd party audience management to measure the impact of online adverts should be included as an exception for collection of terminal equipment data within Article 8(1). This should include the ability to continue carrying out web analytics to assess the benefit of assessing effective advertising. As an enabler of financing apps or websites, the functioning of the digital economy would be adversely impacted if the proposal rendered it impossible for online advertisers to offer their services. In fact, it would tilt the level playing field towards larger businesses with in-house online advertising services.

Further legal clarity is needed within Article 8 to determine what data and devices are covered. Businesses need clarity within law in order to remain compliant. It is currently unclear which *"end-user"* is covered within Article 8(1). This could be better aligned with the GDPR to instead refer to the *"data subject"*. Is this personal content and non-personal metadata? Article 8(2) is also unclear as to what is meant by *"collection of information"*. Does this also cover M2M communications similarly to Article 6 with regard to electronic communications data? This will greatly impact the Commission's wider objectives to digitalise industry.

5. Privacy Settings

BusinessEurope fully supports the use of meaningful privacy settings for the collection and use of data through software. In practice, businesses already design effective software through experts on the basis of user feedback. Not only is an expert required in this process to determine the most relevant technology for a certain situation, but their latest research is vital to determine how users access their service. As a result, the most up to date evidence based solutions are offered to users of these services that take user experience and high levels of protection into account. This also enables an element of competition between service providers to improve the levels of protection offered.

Article 10 and in particular the related recitals are extremely prescriptive and will not enable businesses to continue offering the best privacy solutions for their users in a competitive environment. Instead, only one method of protection is offered that stipulates how privacy settings are presented to users. This would add burdens to businesses without creating better privacy results.

More broadly, Article 10 would result in a sharp increase in third-party cookie-blocking. Users will be required to make a choice on their privacy settings immediately following the download of a software. In this context, users will not appreciate the implications of

the choice they are making because they have not yet begun to use the services for which these technologies are required. This will have a severe impact on businesses that rely on third parties and their technologies. Smaller publishers that outsource management of their adverts to third parties, which is something all small publishers must do to monetise their websites, will be particularly effected. This proposal will stifle their ability to compete with larger businesses that do not rely on these third parties.

Article 10 and its corresponding recitals should be deleted and instead handled within the GDPR. It is too focussed on existing technology. It is not technology neutral and will not remain robust enough to encompass future developments. Legislation should only set out the framework and goals for actors to achieve and not dictate the methods of achieving that result. The GDPR already contains provisions on lawful processing and provisions on profiling. It also expressly calls out the use of tracking and monitoring. Furthermore, the proposal will not achieve the Commission's intention of creating a level playing field between providers. Developing a proprietary advertising, web based measuring solution will be impossible for most businesses. More broadly, it will scupper the Commission's intentions to sustain net neutrality. Many businesses will be left with no choice but to fold or charge for their services. As a result, the internet will be filled with paywalls and exist only for people prepared to pay for it. Having browsers set to 'no cookies' by default will cause businesses ask the user to enable them, continuing the proliferation of popups. Cookie banner removal will not be achieved by the Commission as Article 10 creates obligations for any software permitting electronic communication to give consumers information on consent and privacy settings. In practice, this means the consumers online shop experience will deteriorate as development would move towards mandatory login accounts for online shops.

6. Law enforcement access

BusinessEurope understands that Member States are responsible for national security and the detection and fight against criminal activities. National law enforcement authorities need the possibility to conduct investigation and collect relevant information to safeguard national security interests. Providers of electronic communications work closely with these authorities to respond to requests in practice on a regular basis. As a result, procedures are built into the business models of many electronic communication providers and services to aid authorities in their response to national security threats.

Yet as Article 11 refers to Article 23(1)(e) of the GDPR, the current restrictions of fundamental rights and freedoms in relation to national security, defence, public security and the prevention of crime will be expanded, to also cover economic or financial interests of Member States. This will broaden Member States' authorities access to data in the fields of taxation, public health or social security matters, without the protection otherwise granted by law.

Furthermore, businesses are not protected from requirements to implement backdoor solutions and weakening their technologies, such as encryption, to enable greater Member State intervention. For online service providers that operate across many Member States, Article 11(2) is also not clear on where jurisdiction would lie in the event of conflicts arising between authority's due to disclosure of data following a request to a business. The ePrivacy Directive, which is built on the stated objectives of ensuring confidentiality of a communication, does not offer any kind of safeguards against such pressure.

Article 23(1)(a)-(d) of the GDPR should apply to Article 11 of this proposal or simply revert to the current language as suggested by the Article 29 Working Party in Opinion 01/2017, point 44. Broadening the possibilities for Member States to override the fundamental privacy rights of citizens could encourage implementation of disproportionate surveillance legislation in practice. This hardly achieves the Commission's overall objectives of enabling greater user privacy and the promotion of confidentiality. In fact, it will greatly restrict the fundamental rights of users for reasons beyond national security and preventing and pursuing crime.

Any requirement that would lead to the weakening of security should be prevented in this proposal. Not only does this go against the intentions of this proposal, but it is out of the interests of businesses to weaken their privacy abilities they offer to users in practice. Sufficient procedures to respond to national authorities while upholding the privacy of users are already built into existing business models.

Further clarification is needed in Article 11(2) with regard to jurisdiction. The Commission should consult and evaluate this area further before provisions are legislated within this proposal.

7. Right to control electronic communications

BusinessEurope agrees that end-users should have the ability to control their reception of electronic communications. This can take place through various mediums. In fact, businesses want to learn how they should efficiently market their consumers. This area of marketing should not be confused with spam. The rules set to govern this area of commercial activity should remain robust enough to stand the test of this rapidly developing technological area. They should also be relevant to the current state of online marketing and the technologies that enable it. The opportunity to simplify and remove out of date legislation should also be taken when the chance arises. Rules should also be harmonised where necessary and create a level playing field.

Including the rejection of anonymous calls seems out of date in an age of smartphones that can easily be managed by the user to block this type of call. **Article 12(1) and 14 should be deleted.** We also understand that national law already applies in many Member States that enables publicly available number-based communication services to override the elimination of presenting call line identification on a temporary basis, yet the recorded use of this possibility is extremely low. **Article 12(1)(b) should be deleted.**

Article 15 would essentially ban telephone books, whereas the current national opt-in or opt-out possibilities across the Member States is already significantly regulated. Further to this, legislating in this area seems irrelevant due to the rise in popularity of search engines to carry out this task. **Articles 15 (1)-(3) should be amended to enable Member States the discretion to continue providing opt-in or opt-out mechanisms to ensure the protection of both natural and legal persons.** Where Member States choose to implement opt-in mechanisms for natural persons, **Articles 15(1)-(2) should be brought in line with the GDPR through simplifying the consent procedure for such persons.** Additional steps should not be needed to to gain consent for each category of data and whether it is searchable. End-users will already have the possibility to amend their data or delete it.

In order to avoid fragmentation of an EU-wide scheme for direct marketing, **Article 16(5) should be deleted and Article 16(4) extended to make it obligatory, not an option for Member States.** This would unleash the potential of market growth and

secure consistency across the EU. It should introduce an opt-out mechanism for direct marketing voice-to-voice calls for all end-users (natural or legal persons). There is no reasonable justification in this area for introducing higher protection in case of legal persons (opt-in) than for natural persons (opt-out).

It is a common marketing practice for business to inform their customers of other products or services they could be interested in. In modern e-commerce, this activity is as similar as placing windows in shops. DPAs have accepted that this ability can sustain once the business to consumer relationship has been created (eg. purchasing of a product with consent to marketing). Yet Article 16(1) and (2) will end this current practice and disproportionality limit it to "similar products" only. It is also legally uncertain as to who will ultimately decide what is a "similar product". **The status quo should be maintained in practice to permit businesses at least one year to sustain the consent granted** to carry out these marketing practices. This would be more relevant for modern e-commerce that relies on this promotional activity to maintain and gain customers, particularly SMEs.

Such online tools that do not require consent, eg. banner ads, newsfeeds and pop-up ads, should not be confused with true direct marketing practices that require consent, eg. direct mail, direct messages or placing on social media outlets. This consent is often achieved through technical settings of a software application that enables access to the internet. **Article 16 should further clarify that broader forms of online marketing do not fall under direct marketing practices as they do not target particular individuals.**

8. Security risks

BusinessEurope agrees that transparency is required for users if a personal data breach occurs. The GDPR already sets out the process in Article 31 whereby businesses inform supervisory authorities of a personal data breach within 72 hours and the steps it has taken to mitigate it. Businesses are also required to inform the user of the breach without undue delay as part of this process. As a result, businesses are already taking steps to prepare for the full application of the GDPR from May 2018 onwards to implement this procedure.

Article 17 of this proposal overlaps Article 31 of the GDPR and creates legal uncertainty in the area of user transparency. These provisions are legally uncertain as they stipulate that businesses should *"inform"* users of any risks that *"may"* compromise the security of a service. But this "particular risk" is not defined, neither is what *"may compromise"* means and who makes that assessment?

There is also an overlap with the NIS (Directive on security of network and information systems) as it already covers the situation of triggering, thresholds and roles of informing authorities. NIS lays out certain categories and notification thresholds to distinguish between critical infrastructure and digital service providers. It also points to the requirement for an incident to have significant effects on the business community. These exact thresholds are still being determined in the implementing acts of the NIS.
In practice, this provision would also be overly disproportionate on businesses due to the sheer amount of cyber-attacks occurring on a daily basis. Informing users of each one could lead to a mass of communications, and possibly a loss of focus on the issue. Not to mention disruption of the service itself and the risk to increase eventual additional attacks when the networks and services might be more vulnerable.

Article 17 should be deleted and not transferred to the EECC proposal. Overlap in this area will be too legally uncertain for businesses to fully comply with. In that sense, only after the fact of a breach should notification be made. The roles of actors within this process would then be able to be more clearly defined within this proposal. This also makes sense with the state of best practices within cybersecurity. You would not want to disseminate information of a possible weakness on a network as hackers would be aided to locate that weakness and move in on this target. Further to this, not all potential risks can be practically notified. Users would rather benefit from being informed of serious security breaches rather than mere security risks. Also, would users really benefit from notifications that security events have been handled correctly? Resources would be better placed on being transparent in regard to actual security incidents.

9. Independent Supervisory Authorities

BusinessEurope agrees that legislation should be appropriately enforced by independent supervisory authorities in order to create a level playing field. In fact, it is businesses investing in compliance that want to see strong proportionate enforcement. At the same time, businesses want authorities enforcing the rules to be sufficiently equipped with the knowledge and experience of the policy area to do so.

That is why regulators overseeing this policy area today should be transferred to the national Data Protection Authorities (DPAs). Concentrating responsibility with a single authority is beneficial for consistency and simplicity. This will benefit businesses as they would only have to relate to one authority. It will also decrease the risk of inconsistencies. Furthermore, gathering resources in this manner will increase flexibility in assigning resources to relevant enforcement actions. If no significant privacy issues can be identified in this area, employees can be assigned to work on challenges in others.

Art 18 should grant all enforcement powers to DPAs. It is important that enforcement is not only carried out in a resourceful manner but that alignment with the GDPR is sought so that businesses also have a single contact with regard to enforcement in this policy area.

10. Remedies

BusinessEurope understands the importance of granting the abilities to users to seek remedial redress in the occasion of breach of legislation. Within Article 80 of the GDPR this is possible, even with the ability to be represented by another not for profit organisation.
Article 21 redefines such a class action system, offering a different interpretation. It will apply to any natural or legal person other than the user that was adversely impacted by possible infringements.

Article 21 should be deleted. As rules are already covered in this regard in the GDPR, a simple reference to them would achieve the Commission's objectives of building on the GDPR. It would also mean greater legal certainty for businesses in practice who would operate both under this proposal and the GDPR.

* * *