EUROPEAN
COMMISSION

Brussels, 10.1.2017
SWD(2017) 3 final

PART 3/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

{COM(2017) 10 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

ANNEX 8: DRAFT ECONOMIC ANALYSIS REPORT BY DELOITTE (SMART 2016/0080)

Economic Analysis

Introduction

This Annex, provided by the Commission's contractor of the external study supporting the impact assessment (Deloitte)[117], serves to achieve two objectives:

- To outline the overall model used for the projections, incl. a transparent discussion of its strengths and areas of further improvement ideally necessary[118];
- To present and explain the qualitative and quantitative data and assumptions used for the projections (incl. the specific approach used to translate qualitative reasoning concerning the assessment of the impacts of the policy options into tangible, quantitative assumptions).

A separate section is devoted to each of these objectives.

The overall model used for the projections

This section outlines the key procedural / analytical steps of the model developed for the assessment of the problem assessment, the establishment of the baseline scenario, as well as the assessment of the policy options and their comparison with the baseline scenario.

In addition, the section identifies key strengths and weaknesses of the model.

Overall, the model serves to provide quantitative projections as of 2002 until today. This can both be used for the REFIT exercise, as well as for the assessment of the problems. In addition, the model serves to provide quantitative projections for the expected development until 2030. These projections inform the establishment of the baseline scenario, and the quantitative assessment of the impacts of the options compared to the baseline scenario (status quo).

Key procedural / analytical steps of the model

Based on a number of assumptions that are further elaborated below (section 4), the model is used to project:

- The number of citizens affected by the ePD in the EU and per Member State between 2002 and 2030;

[117] Deloitte, Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector (SMART 2016/0080).

[118] As will also be shown below, the projections should not be regarded as "exact calculations" but rather as projections based on (very) limited quantitative data in relation to what the situation is today, what it was before, and what it will be in the future.

- The number of businesses (per size class) affected by the ePD in the EU and per Member State between 2002 and 2030;
- The magnitude of compliance costs for these businesses per year and Member State, as well as per size class; and
- The magnitude of costs stemming from administrative burden for businesses per year and Member State, as well as per size class.

Within the model, each of the above is projected based on distinct steps. These steps are presented in the table below.

Table 1 – Quantitative assumptions used for the projections

	Number of citizens affected	Number of businesses affected	Magnitude of compliance costs	Magnitude of costs from admin. burden
Preparatory tasks				
Step 1	Identification of relevant Eurostat data and evidence concerning the current usage rate of the services covered.	Identification of relevant Eurostat data	Identification of relevant quantitative economic data needed for the projections (see "basic assumptions" above). *[Eurostat data on the number of businesses is re-used]*	
Step 2	Projection of Eurostat data back to 2002 and until 2030 based on the CAGR of the identified data set (incl. completion of gaps in the initial Eurostat data set). Projection of the available evidence on usage rates of services back to 2002 and until 2030 based on the respective CAGRs	Projection of Eurostat available data back to 2002 and until 2030 based on the CAGR of the identified data set (incl. completion of gaps in the initial Eurostat data set).		
Step 3	Definition of qualitative assumptions regarding the development of the number of citizens and businesses affected, as well as compliance costs and costs related to administrative burden under the policy options and translation of these assumptions into quantitative proxies concerning the increase / decrease in the figures (in % per Article of the ePD) in the baseline scenario under each policy option.			
Milestone 1: Preparatory tasks are completed				
Assessment of the problem and establishment of the baseline scenario				
Step 3	Multiplication of Eurostat data concerning the number of citizens per year and Member State with the projected usage rates for each type of service.	Multiplication of the number of businesses per year, Member State, and size class with the share of businesses that have a website per size class.	*Cannot start before Step 4 concerning the number of businesses is completed because this is used as the relevant statistical basis.* Multiplication of the number of affected businesses per year, Member State, and size class with the share of websites that use cookies and that comply with legislation (e.g. because the websites are not inactive). Projection of a minimum, medium, and maximum scenario.	*Cannot start before Step 4 concerning the number of businesses is completed because this is used as the relevant statistical basis.* Multiplication of the number of affected businesses per year, Member State, and size class with the frequency of information obligations per year and with the hours of work of respective tasks.
Step 4	n/a	Multiplication of the number of businesses per year, Member State, and size class with the share of businesses that use cookies. Projection of a minimum, medium, and maximum scenario.	Multiplication of the number of websites that comply per year, Member State, and size class of business with the costs for websites to be compliant in EUR. The costs for websites to be compliant include costs related to Art. 5(3) and Art. 13. Costs related to Art. 4, as well as Arts. 5(1) and 5(2) have also been / are / will be incurred but cannot be estimated due to a lack	Multiplication of the number of hours per year, Member State, and size class of business with the average salary in the EU in EUR. *Simultaneously:* Calculation of the Present Value of these costs in 2016.

	Number of citizens affected	Number of businesses affected	Magnitude of compliance costs	Magnitude of costs from admin. burden
			of data.[119] Therefore, the estimates are very likely to underestimate the actual value of compliance costs. *Simultaneously:* Calculation of the Present Value of these costs in 2016.	
Milestone 2: Both the problem assessment (2002-2015) and the baseline scenario (2016-2030) are established.				
Projection of figures under the policy options and quantitative assessment of policy options				
Step 7	Multiplication of the baseline scenario figures per year and Member State with the expected increase / decrease of the number of affected citizens in % in relation to provision of the ePD, and each type of service per policy option.	Multiplication of the baseline scenario figures per year, Member State, and size class of business with the expected increase / decrease of the number of affected businesses in % in relation to each provision of the ePD per policy option.	Multiplication of the costs per year, Member State, and size class of business in the baseline scenario with the expected increase / decrease in % under the policy options based on a qualitative assessment of the impacts of each element of the policy options (see above).	
Step 8	Comparison of the policy options with the baseline scenario to identify a preferred policy option.			
Milestone 3: The quantitative assessment of the policy options and their comparison with the baseline scenario is completed.				

Source: Deloitte

Strengths and areas for improvement of the model

As part of this study, a pragmatic approach based on a model has been taken, compared to, for example, a regression analysis. The purpose of this section is to outline why this decision has been taken by addressing – in an open and transparent manner – strengths and areas that could be improved in case better data would be available.

Overall, the development and application of a certain type of economic model always depends on the types, granularity, and usefulness of the data available. Hence, economic modelling is always a trade-off between three factors: (1) The level of detail and accurateness of the model; (2) The accessibility of the model for outsiders and non-experts; and (3) The proportionality of the efforts to gather the relevant data, and to develop and implement the model in view of its usefulness for the analysis.[120] This means that modelling is always about striking the right balance between these factors.

Strengths of the model:

- The model is constructed in such a way that projections are "reasonable based on the information available and the assumptions made" – even though it has not been possible to gather comprehensive quantitative data (e.g. relating to *all* provisions), in particular with regard to any types of micro- and macro-economic costs.

[119] Costs concerning other Articles, are expected to be comparatively insignificant today and/or have already been written off since the adoption of the ePD in 2002.

[120] According to the Better Regulation Guidelines (see section 2.5.3, page 27), only the most significant impacts should be quantified if possible, i.e. if they are susceptible of being quantitatively estimated through a sound methodology and if the required data exists and can be collected at a proportionate cost.

- The model provides a pragmatic approach of projecting quantitative (economic) data that would otherwise not be available into both past and future.
- The model uses only a limited number of clearly defined assumptions, which makes it easy to adjust the projections in case better data becomes available. Given the lack of quantitative data, the assumptions made are considered to be fairly robust, given that minimum, medium, and maximum scenarios have been used to project ranges where appropriate.
- The limited number of assumptions also makes the model more understandable to outsiders. This makes the model's results traceable also for non-experts.
- The model allows for a quantitative comparison of the policy options with the baseline scenario based on clear and traceable assumptions on how the policy options have an impact on the quantitative data.

Areas in which improvements could be made in case better data was available:

- In relation to costs for businesses, the model only projects the available data on compliance costs and costs stemming from administrative burden": (1) This means that, although efforts have been undertaken to obtain more and better data from businesses and business associations, the data used in the model is the best data available. (2) This means that opportunity costs (e.g. from lost business opportunities) are not in scope of the model, although they are assessed qualitatively. This has two reasons: (1) Only illustrative quantitative evidence is available; and (2) A sound quantification of future opportunity costs (e.g. until 2030) is hardly feasible because they depend on the market success of future technologies and business models that are not yet developed (or even conceived) today. What is possible, however, is the qualitative illustration of current opportunity costs.[121]
- Feedback received from businesses shows that after the adoption of the ePD, businesses incurred significant capital expenditure (CAPEX) to develop and implement the technical measures needed to comply with the legislation. The model implicitly assumes that such historical capital expenditures to comply with the ePD (CAPEX) in particular for technologies and services outdated today have been written off already by the businesses and have amortised themselves over the years. This concerns, for instance, costs regarding the presentation and restriction of calling line identification which is already built-in by design in modern devices today. Recurring operating expenditures (OPEX) are assumed to have decreased over time with only insignificant recurring costs occurring today. Due to the lack of data on such historical costs, however, they cannot be projected. The result is that the compliance costs for businesses projected for the time period directly after the adoption of the ePD are likely to be underestimated.
- With regard to some of its elements, the model does not apply dynamically, i.e. accounting for evolving variables over time, but rather static assumptions regarding

[121] A 2016 study by the Open Rights Group, for instance,[REFERS TO ANOTHER STUDY WHICH] estimates that that by 2016 UK mobile operators could be making over half a billion pounds a year just from monetising the location of their customers. In terms of opportunity costs, this means that if such direct monetisation would depend on the prior consent of consumers, UK mobile operators alone (i.e. not the retailers who could monetise location data of their customers) could miss roughly 600 million Euro per year in revenue. See: https://www.openrightsgroup.org/assets/files/pdfs/reports/mobile-report-2016.pdf

the quantitative value of the variables. This means that, due to a lack of data, the model assumes that the following variables included in the model are stable over time (2002-2030):

- The share of businesses that have a website;
- The share of websites that use cookies;
- Similar average wages across the EU in relation to information obligations; and
- The number of working hours per task in relation to information obligations, as well as the frequency of obligations.

Ideally, the model should apply dynamic quantitative figures (i.e. evolving over time) for all these elements and, in addition, account for inflation in relation to pricing developments. With the Net Present Value, we have however used a measure that allows to project values in 2002 (e.g. the costs related to administrative burden) based on constant prices of 2016.

A similar point is valid for the assessment of the policy options. The model assumes consistent impacts of the policy options over time (i.e. percentages of increases / decreases of the number of citizens and businesses affected, as well as the costs for businesses).

Overall, the use of such a *pragmatic* model is reasonable both in view of the given data limitations and the focus of the analysis as such. Finally, the based on the model it is possible to project at least some quantitative data and thus add value to the overall analysis.

The qualitative and quantitative data and assumptions used for the projections

This section presents the available quantitative data, as well as the underlying quantitative and qualitative assumptions with regard to the REFIT exercise, the assessment of the problem and the establishment of the baseline scenario. The assumptions concerning their impact of the policy options on the quantitative elements identified in the bullet points above are presented in a separate table below.

Basic assumptions for the problem assessment and the establishment of the baseline scenario

In general terms, quantitative economic data as concerns most aspects surrounding the ePrivacy Directive are scarce. Feedback from businesses received as part of the online survey and the interviews carried out shows that:

- The vast majority of the organisations consulted do not hold quantitative information concerning the impacts of the ePD, e.g. as concerns the relevant costs (meaning compliance costs, costs stemming from administrative burden, and opportunity costs); and
- In case quantitative information is available, it is patchy, mostly anecdotal (i.e. not available in a structured sense), inconsistent, inhomogeneous, and inconclusive (meaning that information from one stakeholder can be contradictory to information from another stakeholder).

In order to mitigate this challenge, a pragmatic, quantitative model that is based on a limited set of quantitative building blocks has been developed. More specifically, the model is based on two types of data:

- Publicly available Eurostat statistics on the number of citizens (2002-2015) and businesses (mostly 2010-2014) per year and Member State; and
- Quantitative data obtained by means of desk research, the online survey, and the interviews carried out. As indicated above, the available data is scarce.

While the Eurostat statistics have been used as the primary building block for the projections, the data gathered as part of the desk research, the online survey, and the interviews have been used to develop the assumptions on which the projections have been carried out.

Table 2 provides an overview of the quantitative assumptions used for the projections. Table 4 provides more detailed explanations of these assumptions, as well as qualitative reasoning.

Table 2 – Quantitative assumptions used for the projections

Information need for which a quantitative assumption has been made	Quantification
Number of citizens affected	
Compound Annual Growth Rate (CAGR) for services (2016-2030)	%
Internet to browse online	3.4%
Online social networks	3.4%
E-Mail	4.0%
Instant messaging	7.9%
VoIP	9.7%
Mobile phone to make calls or send texts	3%
Fixed phone line	-4%
Number of businesses affected	
Constant shares of businesses that have a website by size over time	
0 to 9 persons employed (micro-enterprises)	60%
10 to 19 persons employed (SMEs)	75%
20 to 49 persons employed (SMEs)	75%
50 to 249 persons employed (SMEs)	85%
250 persons employed or more (large enterprises)	95%
Share of non-EU businesses that have a website[122]	99%
Share of websites using cookies	
Maximum scenario	55%
Medium scenario	50%
Minimum scenario	45%

[122] Non-EU businesses that are active in the EU and have websites fall under the ePD. Therefore, it is important not to discard them as part of the quantitative assessments.

Information need for which a quantitative assumption has been made	Quantification
Compliance costs	
Share of websites that would need to comply	
Maximum scenario	47%
Medium scenario	42%
Minimum scenario	37%
Costs for websites to be compliant	900 EUR
Average useful life time of a website in years	3 years
Costs (EUR) per website to be compliant (one-off)	300 EUR
Share of businesses that have a website and use cookies and potentially provide for unsolicited communication using publicly available electronic communications services in public communications networks	90.0%
Additional share of annual costs for websites to be compliant	25.0%
Additional annual costs for websites to be compliant	75 €
Frequency of checking the Robinson list (per year)	26.0
Duration of checking Robinson list	15 minutes
Social discount rate for Net Present Value	4%
Administrative burden	
Average salary per hour	18 EUR
Number of hours consumed with an information obligation	
Maximum scenario	16 hours
Medium scenario	8 hours
Minimum scenario	4 hours
Frequency of information obligations per annum	
Maximum scenario	Once every two years
Medium scenario	Once every four years
Minimum scenario	Once every eight years

Source: Deloitte

In addition, below a mapping is provided in relation to the types of businesses (i.e. only businesses active in the telecommunications sector or potentially businesses in all sector) covered by the analysis in relation to each of the ePD's provisions as part of the REFIT exercise, the problem assessment and establishment of the baseline scenario, as well as the assessment of the impacts of the policy options compared to the baseline scenario.

Table 3 – Mapping of types of businesses covered by each provision of the ePD

Article	REFIT exercise	Problem Assessment	Baseline scenario	Assessment of policy options
4.1 & 4.2	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector with emphasis on additional OTTs
4.3 & 4.4	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector
5.1 & 5.2	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector with emphasis on additional OTTs
5.3	All businesses that store or access information in the users' terminal equipment (e.g. based on cookies)	All businesses that store or access information in the users' terminal equipment (e.g. based on cookies)	All businesses that store or access information in the users' terminal equipment (e.g. based on cookies)	All businesses as above with emphasis on additional browser providers, app store providers, and

Article	REFIT exercise	Problem Assessment	Baseline scenario	Assessment of policy options
				operating system providers
6 & 9	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector with emphasis on additional OTTs
7	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector
8 & 10	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector
11	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector
12	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector
13	All businesses that provide for unsolicited communications by means of electronic communications	All businesses that provide for unsolicited communications by using publicly available electronic communications services in public communications networks	All businesses that provide for unsolicited communications by means of electronic communications	All businesses that provide for unsolicited communications by means of electronic communications

Source: Deloitte

Table 4 – Qualitative and quantitative assumptions used for the projections

Broad area of assumption	Assumption and brief explanation
Number of citizens affected	
General assumption on the future growth of the population	The past and future growth of the population follows the growth rate of the years for which data is available, e.g. 2002 to 2015 (per Member State, based on Eurostat data). This is a common assumption for models projecting future scenarios. However, it is a rather static assumption that does not take account of e.g. national population policies (in particular regarding fertility and ageing). It should be kept in mind that, under certain conditions such as no *jump* in fertility rates occurs in the future, the population growth might not only be slowing down, but also turn into a decline at some point. Similarly, past population growth could have also been different from in the years for which data is available. However, as no specific data is available, this assumption seems most pragmatic. We have used Compound Annual Growth Rates (CAGR) to project the development of the population into the future. The CAGR represents the year-over-year growth rate (in %) for a specific type of statistics and is used as a multiplicative factor in order to project the figures identified in the problem assessment until 2030 as a cumulative figure, or in 2030 as an annual figure. In order to project a figure in 2030 the following formula has been applied: $y_t = y_{2016} \times (1 + CAGR)^{(t-2016)}$ Whereas y_t is the value of the number of citizens affected in year t, The CAGR can be used to project figures both into the future, as well as into the past in case no relevant public statistics from Eurostat are available.
General assumption concerning the number of citizens affected based on usage rates of services	The number of citizens affected is linked to the (projected) usage rates for each service covered by the ePD. The projections are based on Eurobarometer data[123] regarding the share of citizens that make use of a service "at least a few times per month".[124] This means that only citizens that make use of a specific service are affected – either positively (e.g. benefitting from higher privacy standards) or negatively (e.g. if companies are not compliant), while others not making use of a service are not affected. In practice, however, it could be argued that also citizens that do not make use of a service could be affected. This argument has two components. On the one hand, citizens could use services on behalf of others, e.g. buying products online for elderly, transferring cash online to a regular bank account for which data could be hacked, communication not *with* but *concerning* a third person etc. On the other hand, there is also a societal component, in that e.g. in case of a security breach or data hack, not only the person who has been subject to the security breach or being hacked is affected, but quite naturally also the citizens in the social environment of this person. Such argumentation is, however, not reflected in our projections. We have used Compound Annual Growth Rates (CAGR) to project the development of the usage rates in the future (see also below).

[123] Flash Eurobarometer Survey 443 on ePrivacy.
[124] In addition, account has been taken of the approx. years in which major OTTs (WhatsApp, Facebook, and Skype etc.) were introduced in the EU markets. This means that usage rates increase by a larger margin since then.

Broad area of assumption	Assumption and brief explanation
Compound Annual Growth Rate for services reflected in Flash Eurobarometer 443	
Internet to browse online	We have used a **CAGR of 3.36%** for this service. This assumption is based on evidence regarding the increase of global consumer Internet traffic (2015 to 2020), which is estimated to be 18%.[125] Assuming an unchanged growth rate for the time frame of 2020 to 2030, the respective CAGR can be calculated.
Online social networks	See *Internet to browse online*
Email	We have used a **CAGR of 4%** for this service. This assumption is based on evidence regarding the increase in mobile email traffic by 32.8% from 2010 to 2015.[126] As this is the best data available, it is assumed that this forecast also applies to the timeframe of 2015 to 2030. However, it is assumed that the actual CAGR is likely to be lower. The reason for this is that emails are expected to be gradually replaced / complemented by other forms of communication such as instant messaging – in particular in the private sphere but also more and more in a business environment. Therefore, the projected development can be considered as a maximum projection.
Instant messaging	We have used a **CAGR of 7.92%** for this service. This assumption is based on evidence regarding the increase in mobile IM traffic by 46.3% from 2010 to 2015.[127] As this is the best data available, it is assumed that this forecast also applies to the timeframe of 2015 to 2030. However, it is assumed that the actual CAGR is likely to be lower because of new future market developments that might evolve further from instant messaging. Therefore, the projected development can be considered as a maximum projection.
VoIP	The global VoIP volume is expected to **grow by 9.7%** between 2014 and 2020 by Transparency Market Research.[128] It is assumed that this estimate to be applicable as a CAGR for the number of VoIP users.
Mobile phone to make calls or send texts	No evidence could be found on the CAGR in relation to this service. However, it is assumed that, in line with general market trends such as the increased use of mobile devices and mobile internet, the use of mobile phones to make calls or send texts will increase by a **CAGR of 3%.**
Fixed phone line	In 2010, IBM calculated a voice traffic **decline in minutes by 4%** between 2003 and 2008. This information is used to project the development until 2030, keeping in mind that the decline could be even stronger based on the take-up and development of other services.
Number of affected businesses	
General assumption on the future growth of the number of businesses	Similar to the number of citizens, the past and future growth of the number of businesses (micro, SMEs, large, and foreign enterprises) is expected to follow the growth rate (overall) of the previous years (per Member State, based on Eurostat data). We have also used Compound Annual Growth Rates (CAGR) to project the development of the number of businesses in the future based on available public data from Eurostat.

[125] See: http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf, page 14.
[126] See: http://www.telecomsmarketresearch.com/reports/itm_Mobile_Messaging_extract_LR.pdf
[127] See: http://www.telecomsmarketresearch.com/reports/itm_Mobile_Messaging_extract_LR.pdf
[128] See: https://www.linkedin.com/pulse/20140911043449-339157087-voip-services-market-is-growing-at-a-cagr-of-9-7-from-2014-to-2020

Broad area of assumption	Assumption and brief explanation
General assumption concerning the number of businesses affected by the ePD	For the calculation of the compliance costs of the ePD, it is assumed that the ePD potentially affects all businesses that run a website and use cookies based on Article 5(3). The number of businesses affected by other provisions of the ePD is expected to be significantly lower as they refer to the telecom market only (e.g. Art. 4, 5(1), 5(2)) or only to a sub-group of businesses (i.e. those providing for unsolicited communication using publicly available electronic communications services in public communications networks under Art. 13 – this means that not all businesses that you "some sort of communication B2B or B2C" are covered but only those that make actual use of "unsolicited communication".)).[129] Overall Article 5(3) extends the scope of the ePD also to businesses active in other industries than the telecom sector.[130] Keeping this in mind, alternative projections have been carried out for businesses that Eurostat strictly defines as being part of the "Telecommunications sector", i.e. businesses providing telecommunications and related service activities, such as transmitting voice, data, text, sound and video. While the former projections concerning "businesses overall" can be regarded as projections of the absolute maximum values, projections referring to the "telecommunications sector only" should be seen as minimum projections.
General assumption concerning the application of Art.5(3) to potentially all businesses	We assume that Article 5(3) generally applies to all businesses that operate a company website, as cookies can be stored and information can, in principle, be tracked on every website. However, there are two important restrictions to this assumption: (1) Not all businesses run a website; and (2) Not all company websites use cookies (i.e. "no cookies" vs. "some sort of cookie"; If a website does not use any cookies, they do not need to comply. If they are using any sort of cookies, they indeed need to comply). Hence, it can reasonably be assumed that the maximum number of businesses in the EU affected by the ePD has a strong correlation to the number of company websites operated by: (1) Businesses that have their primary place of establishment within the 28 EU Member States; and (2) Third-country businesses that operate within the EU (i.e., by means of their own website(s)). With regard to the share of websites using cookies, projections have been carried out in relation to three scenarios (minimum, medium, maximum). In general, the available evidence has been used to project the medium scenario, but have also run projections for a higher and lower scenario in order to account for uncertainty factors around the share of websites using cookies.
Art. 5(3): Shares of businesses that have a website	
0 to 9 persons employed (micro-enterprises)	The share of micro-enterprises that have a website is not available, but it can be assumed that it is below 75% (as for SMEs), since micro-enterprises may be less active online in order to concentrate better on their core business. This does not say that the core business of micro-enterprises cannot be online-based. However, the overwhelming majority of micro-enterprises consists of local shops, small/medium restaurants, and other types of shops that do not necessarily have to have a website in order to be able to provide their products or services. Moreover, the use of general platforms or social networks like Facebook, Youtube, Resto.be, etc. as an alternative to fully-fledged websites is has become widespread Thus, it is assumed that the **share of micro-enterprises that have a website is 60%.**
10 to 19 persons employed (SMEs)	According to Eurostat's latest available data, in 2013, **75% of all enterprises** employing 10 or more persons in the 28 EU Member States had a website.[131]

[129] With specific regard to Art. 13, it should be noted that the number of businesses affected is independent of Member States having enacted an opt-in or opt-out solution in national legislation, as e.g. the Robinson lists are checked by each business anyway on a regular basis.
[130] Overall, the model estimates costs for businesses in relation to Art. 5(3) and Art. 13. Information on costs in relation to other Articles is generally scarce and has, as much as possible, been reflected in the report qualitatively.
[131] [isoc_ci_eu_en2]. Last updated on 9 June 2016.

Broad area of assumption	Assumption and brief explanation
20 to 49 persons employed (SMEs)	
50 to 249 persons employed (SMEs)	We assume that the share of businesses of this size class that operate a website is higher than 75%. However, no quantitative data is available. Nevertheless, it has been **assumed that the share is 85%.**
250 persons employed or more (large enterprises)	We assume that the share of businesses of this size class that operate a business is higher than 75%. However, no quantitative data is available. Due to the size of such businesses, it has been **assumed that the share is 95%.**
Share of non-EU businesses that have a website	Non-EU businesses are by definition active across borders and therefore do not only provide domestic services. Therefore, they are very likely to run a website.it is assumed **that the share is 100%**
Art. 5(3): Share of websites using cookies	
Maximum scenario	As indicated above, minimum, medium, and maximum projections have been carried out based on the share of websites using cookies. **The medium value, for which evidence is available, is 50.2%** based on information by W3Techs who run web technology surveys[132] ("50.2% of all websites use cookies"). In addition, the European Commission's 2015 Article 29 cookie sweep action[133] showed that only 70% of websites with cookies were using tracking cookies. However, as concerns the baseline scenario, such tracking cookies are not relevant for the estimate of the compliance costs but only for the assessment of the impact of the policy options as currently all types of cookies used on websites trigger the cookie notification. We have added / subtracted 5% for each the minimum and maximum scenario in order to project a corridor in which the *actual* figure is most likely to be in (i.e. 40% in maximum and 30% in minimum respectively). This is used as a sensitivity analysis.
Medium scenario	
Minimum scenario	
Compliance costs	
General assumption concerning the *origin* of compliance costs related to the ePD	In general, information on costs incurred in order to comply with the ePD is scarce. Businesses nor business associations only have patchy, anecdotal information on the costs related to the ePD in general. Information on particular provisions is even less available. However, feedback received as part of the interviews suggests that the majority of costs for the ePD is related to: • Art. 4 on the security of processing; • Art. 5(1) and Art. 5(2) on confidentiality of communications; • Art. 5(3) on cookie consent; and • Art. 13 on unsolicited communication. In relation to Art. 4, as well as Art. 5(1) and Art. 5(2), businesses have indicated that they have incurred a significant amount of compliance costs after the adoption of the ePD. However, businesses were not able to provide any quantitative information on this as the costs were already incurred in the past (almost 15 years ago) and have

[132] https://w3techs.com/technologies/details/ce-cookies/all/all
[133] See: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp229_en.pdf

Broad area of assumption	Assumption and brief explanation
	since then been written off. However, businesses indicated in qualitative terms that they incur still today (and will in the future) costs in relation to regular updates, maintenance, and repair of the necessary hard- and software to safeguard the security and confidentiality of communications. However, it was not possible to obtain any quantitative information from businesses on the magnitude of such costs. Art. 5(3) is expected to be responsible for a significant amount of compliance costs. This is due to the extensive coverage of this provision (potentially all businesses in the EU that run a website and use cookies), as well as its importance for today's communication, marketing, advertising, and sales techniques. As businesses are increasingly developing data-driven business models, the importance of the substance of Art.5(3) is also expected to grow over the next years. The costs associated with this provision mainly stem from the need to collect users' consent to be able to use cookies on websites, i.e. to implement the relevant technical solutions on websites. In addition, Deloitte has been requested to undertake particular efforts to estimate compliance costs in relation to Art. 13 on unsolicited communications as this provision, in addition to covering voice calls, also involves the implementation of a technical solution on websites to collect users' consent to *unsolicited* communication. As only very limited quantitative information was obtained from businesses, expert judgment was used to estimate respective compliance costs (see the assumptions below in the section on the assumptions). Finally, after the adoption of the ePD, in particular telecommunication service providers have – according to our interview results – incurred high capital costs in relation to the implementation of: • Articles 6 and 9 on traffic data and location data other than traffic data; • Article 7 on itemised billing; • Article 8 on control of connected line identification (incl. Art. 10 on exception); and • Article 11 on automatic call forwarding. Under Art. 6 & 9, and 12 concerning directories of subscribers, businesses incur some costs regarding information obligations to consumers. Based on the feedback received, these costs can be expected to be fairly large. However, these costs, which were incurred in the past by telecommunication service providers, can be expected to be already written off. Initially high investments have already amortised themselves over the years. In addition, over time, the operational expenditures in relation to these provisions have decreased and are expected to be insignificant in view of the overall costs incurred by businesses today – keeping in mind that costs are incurred in relation to e.g. maintenance, updates, repair etc. Apart from itemised billing (which today is expected to be a standard process with no additional costs for service providers), the services regulated by these provisions are generally regarded as outdated or built-in by design in devices. Overall, this means that the compliance costs estimated as part of this study are based on costs related to Art. 5(3) and Art. 13 (based on expert judgment). The quantitative findings of the study are thus very likely to underestimate the actual amount of compliance costs incurred in the past, today, and thus in the future (at least for new businesses who have not yet incurred the initial capital costs for implementing these provisions). This is due to the fact that capital and recurring expenditures relating to other Articles than Art. 5(3) and 13 could not be estimated. The available evidence has, however, been taken into account in qualitative terms as much as possible.
Art. 5(3) Share of websites that would need to comply	
Maximum scenario	For the purpose of projecting compliance costs, in addition to the share of websites using cookies, it is also important to account for websites that are not active or not complying with legislation. While all *businesses* that run websites with cookies may potentially be affected, costs are only incurred in relation to those *websites* that
Medium scenario	

Broad area of assumption	Assumption and brief explanation
Minimum scenario	need to comply with legislation, e.g. no holding pages, pay-per-click sites, and private (password-protected) sites. The 2014 ITIF report on the economic costs of the European Union's cookie notification policy cites data by EURid, the European registry in charge of ".eu", indicates that 41.9% of websites in the EU are active and complying with legislation.[134] Similarly to the scenarios concerning the share of websites using cookies, this information is used to project a minimum, medium, and maximum scenario for the share of websites that would need to comply. **The medium value is 41.9%,** while 5% have been added / subtracted respectively to project a corridor in which the *actual* figure is most likely to be in (i.e. 47% and 37% respectively).
Costs per website to be compliant	The projection of the compliance costs relies on the costs per website to comply with legislative requirements. The 2014 ITIF report projections a lump sum of 900 EUR per website incl. costs associated with legal advice, updates to privacy policies, and technical updates to websites. The ITIF study was indeed cited by different stakeholders consulted as part of this initiative, implying that this estimate is considered realistic by these stakeholders. Similarly, an online retailer estimated that the costs relating to the implementation of the cookie banner lie around 1150 Euro per website. This estimate is again very close to the estimated 900 Euro per website, although this online retailer also indicated that additional costs occur to deal with customers who complain about seeing the banner even after consenting (e.g. because they clear their browser history or move to a new browser). However, there were also a few stakeholders that indicated that compliance costs would be significantly higher or lower. For instance, an internet content provider replying to the public consultation indicated that the costs to implement the cookie banner would be relatively small and could be similar to the annual costs of hosting a website. A large IT hardware and network systems company reported significantly higher annual costs: they estimate annual costs for a cookie opt-out tool of ca EUR 280,000, and additional costs of ca EUR 70,000 for a trained resource. Based on the information available, it seems that such high costs only apply to large businesses, i.e. the minority of businesses that need to apply the cookie banner. In addition, the ITIF report indicates, however, that it is expected that costs are higher for larger organisations with more complex web operations. Finally, the ITIF report indicates that the average useful lifetime of a website is three years over which the 900 EUR are incurred. Therefore, the annual **price per website has been set at a lump sum of 300 EUR**, knowing that this is only a very raw estimate based on very limited, but best data available.[135] It is expected that this estimate includes technical and legal advice, as well as regular updates and maintenance of the websites cookie policies.
Art. 13 on unsolicited communication	
General assumption	Although only very limited quantitative information is available in relation to costs associated with Art. 13 (apart from information that eCommerce businesses generally check the Robinson list about every two weeks as part of a standardised process), quantitative estimates were still carried out – mostly based on expert judgment. In general, we assume that compliance costs are incurred not by all businesses that provide for unsolicited communication but only by those that also have a website and use cookies because collecting the consent of users over the counter does not produce costs. There are two reasons for which this can be reasonably assumed: (1) All businesses can, potentially, make use of unsolicited communications by electronic communication means– either in a B2B or B2C context. However, it is only those businesses that provide for a website that are actually able to collect users' consent, either by an opt-in or opt-out solution. Furthermore, such businesses are generally expected to make also use of cookies in order to understand better "who their customers are" with a view to providing *targeted* unsolicited communication by electronic

[134] See: http://www2.itif.org/2014-economic-costs-eu-cookie.pdf, page 4.
[135] In fact, the ITIF report itself indicates that the 900 EUR number was chosen based on *feedback from European colleagues* and *personal correspondence with a European think tank*.

Broad area of assumption	Assumption and brief explanation
	communication means. (2) Businesses that provide for unsolicited communication by electronic communication means but do not make use of a website are not able to collect the consent of their customers – both from a B2B and B2C perspective. Therefore, such businesses are expected to simply provide for unsolicited communication – even though this may not necessarily be compliant with national law. In any event, though, the compliance costs incurred by such businesses (e.g. related to legal advice) are (1) expected to be insignificant in view of the overall amount of costs; and (2) even though businesses may have costs related to legal advice, they could still make use of unsolicited communication as the chances of being detected of non-compliance are close to zero. In a nutshell, the compliance costs associated with Art. 13 are thus only incurred by businesses that also incur costs in relation to Art. 5(3). Based on the feedback received from businesses and business associations, three main cost elements can be distinguished in relation to Art. 13[136]: • The technical implementation of the opt-in / opt-out solution; • Checking the Robinson list for B2B and B2C customers that have registered; and • Assisting B2B and B2C customers to register / de-register on such a list. As available evidence is very scarce, estimates are only possible with regard to the first two of the above cost elements. Overall, it has to be kept in mind that the most significant cost element in relation to Art. 13 is not the compliance costs but the opportunity costs – i.e. the costs businesses would incur / the revenue businesses would lose in case they were not allowed to provide for unsolicited communication.
Share of businesses that have a website, use cookies, and potentially provide for unsolicited communication by means of electronic communication	No quantitative information is available in this regard. Deloitte is still making efforts to validate the assumptions with businesses. We assume that almost all businesses that have a website and use cookies could potentially provide for unsolicited communications by electronic communications means – in either a B2B or B2C context. Therefore, we have set the share at a value of 90% of respective businesses.
Additional annual costs for websites to be compliant	No quantitative information is available in this regard. Deloitte is still making efforts to validate the assumptions with businesses. There are some costs associated with the technical implementation of the opt-in / opt-out solution on businesses website. As businesses were not able to provide such quantitative information though, an estimate of an additional share of 25% of the costs per website to be compliant (see above) – i.e. 25% * 300 EUR = 75 EUR, has been assumed per business in order to provide for the respective technical solution on a website.
Frequency of checking Check Robinson list (per year)	As part of an interview with an eCommerce business association, we have received the information that eCommerce businesses generally check the Robinson list every two weeks as part of automated standard processes that only trigger further work in case a B2B or B2C customer has registered on the Robinson list and may thus not be targeted by means of unsolicited communication anymore. Given that the year has 52 weeks, we have set the value therefore at 26.

[136] As part of the interviews, feedback was received that businesses e.g. check the Robinson lists irrespective of whether or not a Member State has implemented an opt-out solution because you citizens may opt-in at the start and then afterwards withdraw their consent through an opt-out again. This means that although consumers might need to opt in at the start by default they can still withdraw their consent (even one second after they opted in theoretically).

Broad area of assumption	Assumption and brief explanation
Duration of checking Robinson list	No specific quantitative evidence was obtained as part of the interviews on the duration of checking the Robinson list. However, it was indicated that this is more or less an automated standard procedure. Without further quantitative evidence available, we assume that it takes an average business therefore not more than 15 minutes to check the Robinson list on a given occasion. For the purpose of the quantification of the costs associated with checking the Robinson list, we have used an average salary of 18 EUR (see the section on administrative burden below).
Overall compliance costs related to Arts. 5(3) and 13	Based on our assumptions outlined above, a given business is expected to have incurred approx. 490 EUR in 2016. This estimate is a recurring cost. However, the magnitude of the costs is decreasing. This means that in 2002, the amount in Euro incurred was higher than today while it is expected to be lower in 2030. The cost Is decreasing because businesses adapt and learn over time and get more acquainted to a certain set of legislative rules. This is closely connected to "economies of scale" in which a solution, once developed and implemented, can be re-produced and adapted at relatively low cost. This has been estimated in the following way: *Art. 5(3):* • Costs per website to be compliant: 900 EUR • Average life time of a website: 3 years • Costs per website to be compliant per year: 300 EUR *Art. 13:* • Additional annual costs for websites to be compliant: 25% of costs per website to be compliant with Art. 5(3) per year • Frequency of checking Check Robinson list (per year): 26 • Duration of checking Robinson list: 15 minutes (i.e. 0.25 hours) • Average salary in the EU: 18 EUR per hour *Formula applied:* (900 EUR / 3 years) + 25% * (900 EUR / 3 years) + 26 * 0.25 * 18 EUR = **490 EUR** *Expected development of costs:* It is expected that the value of costs incurred by businesses per year in 2016 has decreased since 2002 and will further decrease until 2030.

Broad area of assumption	Assumption and brief explanation
Administrative burden	
General assumption on the average salary per hour	We have set the average labour costs (wages and salaries) per hour concerning website-related tasks at 18 EUR across the EU. This is largely in line with Eurostat data on the average amount of wages and salaries in enterprises employing more than 10 persons (excluding other labour costs).[137] Although country-specific differences of course exist concerning the cost of labour, this average amount has been used to estimate costs in relation to each country.
Art. 4: Number of hours consumed with an information obligation	
Maximum scenario Medium scenario Minimum scenario	In addition to the average salary per hour, the projection of the costs stemming from the administrative burden is based on the number of hours it is expected to take one full-time equivalent (FTE) to carry out the tasks related to the information obligations set out by legislation. Under the ePD, information obligations only exist under Article 4 concerning data breach notifications. Such information obligations only apply to electronic communication service providers (i.e. not all businesses as under Art.5(3). Information obligations in relation to provisions other than Art.4 (incl. Art. 4.2 on notifying risks) only exist in relation to an investigation – and are therefore depending on the frequency of enforcement in the specific Member States. The ePD study SMART 2013/0013 has shown, however, that the level of enforcement of most of ePD provisions in most of the Member States is very low.[138] It can be estimated that the overall administrative burden for the application of the ePD provisions, other than Article 4, to be negligible in average terms or in any event very low. Without having received any quantitative evidence from stakeholders – only qualitative information on the duration of related tasks has been obtained – it is assumed (i.e. an assumption, not based on hard facts) for the purpose of this projection that data breach notifications are a standardised electronic procedure (at least within the major market participants' organisations) that, given that national thresholds for reporting are met or exceeded, do not take more than 16 hours per case (i.e. two working days). This has been used as the maximum scenario. Furthermore, the medium scenario has been set to 8 hours per case (i.e. one working day). As a minimum scenario, it is assumed that it takes an FTE 4 hours per case (i.e. half a working day) to process data breach notifications. Since the adoption of the ePD until today, costs in relation to such information obligations are expected to have been mostly occurred by telecommunication service providers. Such costs would decrease further under the Policy Options although the scope of the ePD would be extended to OTTs. However, it has to be considered that none of the policy options provide for regular information/notification obligations for OTTs. Thus, administrative costs would also in this case only materialise in case of enforcement/auditing.
Art. 4: Frequency of information obligations per annum	
Maximum scenario Medium scenario Minimum scenario	In addition to the average hourly wage and the number of hours it takes an employee to carry out tasks in relation to information obligations, the projection of costs related to administrative burden depends on the frequency of information obligations per year. The data received from competent authorities on the frequency of data breach notifications shows that such information obligations are rare, at least on an individual company-by-company basis.[139] For instance, the feedback received (a number of smaller and larger Member States have not provided information on this) indicated that in 2015, 2,915 notifications of personal data breaches were received with number in the years before being (significantly) lower (almost all, 2,867, of these notifications

[137] See e.g.: http://ec.europa.eu/eurostat/statistics-explained/images/a/ac/Estimated_hourly_labour_costs%2C_2015_%28%C2%B9%29_%28EUR%29_YB16.png

[138] See also the Commission Staff Working Document -- Impact Assessment in relation to the GDPR proposal, page 101.

[139] Information obligations in relation to data breach notifications are rare on an individual company-by-company basis – in relation to both subscribers and users, as well as public authorities. This is not due to the non-existence of data breaches but mostly due to the limited severity (i.e. do not affect users' privacy).

Broad area of assumption	Assumption and brief explanation
	relate to the UK and Ireland). Keeping in mind the sheer number of businesses in the EU that could potentially be affected by personal data breaches, we therefore expect that notifications to be a rarity for individual businesses at least.[140] This is also reflected in the 2015 ePD study. The available data on the number of data breach notifications can, however, not be translated directly into a measure for the frequency of data breach notifications per company as it might be that several notifications stem from one or the same company (e.g. relating to one specific data breach or a series of notifications as part of a larger data breach). Despite the absence of further quantitative evidence concerning frequency of data breaches, it is assumed that an individual business would at most have to **report once every two years** (see also the GDPR IAs, NIS impact assessment, and Telecom package IA). The maximum scenario has been set at once every four years, while the minimum scenario has been set at once every eight years. Information obligations concerning data breaches only concern businesses in the telecommunications sector and not all businesses that might otherwise be affected by the ePD, e.g. by Art.5(3).
General assumption concerning projections of costs into the past and future	
Social discount rate for Net Present Value	In relation to costs in the past and the future, it is important to apply discount rates when projecting over a certain time period. The European Commission's Better Regulation Guidelines foresee a standard social discount rate of 4%[141], which has been applied to project the net present value of figures. The Net Present Value (NPV) is calculated in order to make past and future payments over a certain number of time periods comparable to today. This means that e.g. payments in the future would (in the future value of the currency) exceed today's payments, while in today's terms, the payment in the future will actually be lower than today. In addition, according to the Better Regulation Guidelines, "calculating the present value of the difference between the costs and the benefits provides the NPV of a policy measure. Where such a policy or project generates a positive NPV, there would be no obvious reason to prevent it from proceeding, as long as the distribution of costs and benefits among different social groups is deemed to be acceptable and all costs and benefits are included in the computation (which is often methodologically challenging)."

Source: Various sources, tabulated by Deloitte.

[140] In the UK and especially IE there are higher number of security breaches compared to other Member States. However, it can reasonably be assumed that it would be a significant share if seen in relation to the total number of businesses in those countries. As a consequence, this this sentence applies to the whole EU, including UK and IE.

[141] See page 377 of the Better Regulation Toolbox. The Better Regulation Guidelines also indicate that a lower discount rate could be applied for costs in order to account for social benefits achieved through policy intervention. However, for the sake of comparability as emphasised by the Better Regulation Guidelines, 4% have been used.

Approach and assumptions used for the assessment of the policy options

This section presents the assumptions made regarding the impact of the policy options.

The general approach used to translate qualitative reasoning into quantitative assumptions[142]

One of the prime challenges of impact assessments is the translation of qualitative analysis into tangible, quantitative findings. In fact, the Better Regulation Guidelines specify "significant impacts should be assessed qualitatively and, whenever possible, quantitatively." In this respect, "if possible" means that impacts are susceptible of being quantitatively estimated through a sound methodology and if the required data exists and can be collected at a proportionate cost.

Keeping this in mind, an approach consisting of six consecutive steps used is based on a translation of qualitative reasoning of the impacts of the policy options vis-à-vis the baseline scenario into quantitative percentages that are used to estimate in how far the policy options would contribute to an increase or decrease of:

- Number of citizens affected[143];
- Number of businesses affected;
- Compliance costs; and
- Costs stemming from administrative burden.

As a **first step** of the assessment of the policy options, we have carried out a qualitative analysis[144] regarding the potential impact of each element of each policy option:

- What does it mean in practice?
- What types of businesses would be affected? How would the number of affected businesses develop?
- Would these businesses incur (additional) compliance costs and/or costs stemming from administrative burden?
- Would these costs be reduced through the implementation of each element of the policy options?
- To what extent would the policy options contribute to achieving the policy objectives?

[142] There is no explicit methodology to assess the impact on administrations and other economic impact, we have not drafted separate chapters for this.

[143] The number of citizens is a key component of our estimates although it is not subject to change under the policy options (as presented in the main body of the report). The reason why for still keeping this estimate is that it shows that although POs may be introduced, privacy threats to citizens will still exist in the future as the POs change the set-up of how they are dealt with – but do not solve the issue that citizens may be subject to privacy breaches.

[144] As presented above and in the main body of the report, we have used a standard rating scale from -3 to +3 so indeed the ratings are comparable amongst the policy options for each criterion. The criteria itself are naturally not fully comparable with each other (e.g. effectiveness vs. efficiency). The ratings of specific (elements of the) POs are provided in the respective tables in the main body of the report. The main body of the report also provides comparative tables of the POs.

As a **second step**, we have attributed to the answers to each of these questions for each element of the policy options a quantitative rating / colour coding. The purpose of this rating is to compare the magnitude of the impacts on businesses towards each other and to provide the basis for the calculation of possible actual impacts. The rating, thus, provides the qualitative basis for the percentages presented in the previous section. The following scale has been applied:

Significant decrease (-3)	Medium decrease (-2)	Slight decrease (-1)	Neutral (0)	Slight increase (+1)	Medium increase (+2)	Significant increase (+3)

Source: Deloitte

The specific ratings for each element can be found in the coloured cells in each of the tables in the section on the qualitative reasoning.

The scale should be read from left to right: A significant decrease of costs being colour coded green and a significant increase of costs stemming from each element of the policy options being coloured red. The figures in each box represent the quantitative value attributed to each of the ratings with the most negative value having received a -3 and the most positive a +3.

As a **third step**, we have summed up the ratings for each specific element of each policy option in order to provide an overall rating. The overall ratings can be found in the individual assessment tables in chapter 9 of the main body of the report.

The impact of each of the policy options on the number of citizens affected is expected to be 0 as all citizens are affected who use electronic (or online) communication services and/or surf on the internet in general. These citizens are either affected positively (e.g. benefitting from higher privacy standards) or negatively (e.g. if companies are not compliant). This is not changed by any of the policy options: although some of the policy options change the scope in relation to the types of services covered, it is expected that users of online services are also covered under the current situation e.g. as holders of fixed line, mobile phone or internet contracts.[145]

As these qualitative overall ratings of the impacts of the policy options on the number of businesses affected, their compliance costs, and costs stemming from administrative burden are not suitable to estimate in quantitative terms the impact of the policy options, we have used a *hinge (or translation factor, see below)*.

This means that, as a **fourth step**, we have translated the qualitative overall ratings of the impacts of the policy options into quantitative percentages. The percentages represent the impact of the policy options in quantitative terms, i.e. how much a given policy option would increase / reduce the number of businesses affected, their compliance costs, and costs stemming from administrative burden. Such a step is a pragmatic means to cope with the general lack of quantitative evidence concerning the impact of (hypothetical, theoretical) policy options on businesses in the future.

[145] The number of citizens "potentially" affected is always the same across all policy options, as it can always be that – although there are measures in place – citizens are affected by privacy breaches. the question is about the group that is potentially affected, not those that are actually affected (in case of citizens e.g. those that suffer from privacy breaches and in case of businesses those that could actually exploit data for their own purposes).

Each qualitative overall rating has been translated into a minimum and maximum percentage by means of a simple multiplication with a so-called translation factor. This translation factor has been set ad hoc, based on expert prior experience. It has been chosen as the most reasonable to be applied in this case, in light of the subject matter and the type of findings that had to be analysed in this impact assessment. Thus, the translation factor ranges from 0.01 (minimum) to 0.05 (maximum). Hence, if a policy option has for example an overall rating of "+3", the minimum value would be "3%" while maximum value would be "15%", which means for example the compliance costs would rise by a 15%.

The most likely *actual* impact of the policy options is expected to be somewhere within the minimum and maximum value.

Given the specific ratings above, the maximum "translation factor" can mathematically not exceed 0.9 because this would translate the rating concerning the compliance costs under policy option 4 to already 99%. If this policy option was not ranked positively but negatively, for instance -11, the translation factor would result in a decrease of costs by 99%. This can only be exceeded by the total repeal of the ePD – which is the "natural boundary" of impacts. A decrease of compliance costs of more than 100% is logically not possible because it would mean that businesses would not only have less cost but in addition "win something". This is not in line with economic theory.

Therefore, we have used 0.05 as maximum translation factor because it is actually a quite moderate, reasonable, and balanced value. In fact, 0.05 is the median value between 0.01 and 0.09.

The use of a standardised translation factor makes the impacts of the policy options comparable vis-à-vis the baseline scenario, as well as towards each other. Thus, the translation factor is a pragmatic means to cope with the general lack of quantitative evidence concerning the impact of (hypothetical, theoretical) policy options on businesses in the future.

The impact of each of the policy options on the number of citizens affected is expected to be 0%, as explained above. Policy option 5, i.e. the total repeal of the ePD is expected to reduce the number of businesses affected, their compliance costs, and their costs stemming from administrative burden to zero.

The relationship between the percentages presented above represents the expected magnitude of the impact of the different policy options. This means that policy options that have a bigger impact also have a higher (or lower in case of negative impact) percentage. It is important to keep in mind that these assumptions are mainly based on expert judgement, as it was generally challenging to substantiate / validate these with stakeholders. The reasons for this are: (1) Businesses and business associations are focused on the "now". This means that they usually do not have quantitative information on policy options which, to them, are hypothetical scenarios that do not (yet) have a direct effect on their daily operations; (2) Businesses and business associations were able to provide qualitative, anecdotal evidence concerning their costs and how a specific policy option would impact on them. Such evidence has been used to develop the figures above. However, a direct one-to-one translation of qualitative evidence into quantitative estimates is not possible.

Below, we have provided a brief explanation of the assumptions.

- **Numbers of citizens affected**: The number of citizens affected depends on the usage rates of the services. For the baseline scenario, it is assumed that all citizens who use any of the services concerned (including fixed line or mobile phone as well as internet) are potentially affected by the ePD. This is not changed by any of the policy options.
- **Numbers of businesses affected**: For the purpose of the economic analysis, the broadest group affected by the ePD (all businesses that have a website) was taken as a basis. It can be expected that under policy options 3 (at least scenarios 1&2) and 4, the number of businesses affected decreases due to the exceptions implemented under these policy options.
    - **Policy option 1:** This option does not entail any changes that impact on the number of businesses affected by the ePD.
    - **Policy option 2:** Although OTTs would apply additional provisions compared to the current situation, no significant impact on the overall number of businesses (i.e. those applying Article 5.3) is expected. At the same time, the clarification of the scope of the provision and make it technologically neutral may lead to a moderate increase of businesses applying the ePD, as it is clarified that the scope of the provision is technologically neutral and e.g. also applies to companies placing ads on social networks' personal spaces.
    - **Policy Option 3:** Based on the new exceptions, the website that use non-privacy invasive cookies would no longer be affected by the consent rule. Based on current statistics, this would lead to a 30% decrease. Depending on the development in relation to the use of cookies, the actual number could be slightly lower as well. An additional decrease is possible based on the possibility to introduce adequate safeguards. The magnitude of this impact is unknown, as it depends on the types of safeguards employed and the willingness of businesses to implement these. At the same time, Point 5(i) may lead to a moderate increase of businesses applying the ePD, as it is clarified that the scope of the provision is technologically neutral and e.g. also applies to advertisings on social networks' personal spaces.
    - **Policy option 4:** Based on the new exceptions, the website that use non-privacy invasive cookies would no longer be affected by the consent rule. Based on current statistics, this would lead to a 30% decrease. Depending on the development in relation to the use of cookies, the actual number could be slightly lower as well. An additional decrease is possible based on the possibility to introduce adequate safeguards. The magnitude of this impact is unknown, as it depends on the types of safeguards employed and the willingness of businesses to implement these. At the same time, Point 5(i) may lead to a moderate increase of businesses applying the ePD, as it is clarified that the scope of the provision is technologically neutral and e.g. also applies to advertisings on social networks' personal spaces.
    - **Policy option 5:** No business would be affected by the ePD anymore as it would be repealed entirely.
- **Compliance costs**: In relation to policy options 1 and 2, the compliance costs would slightly increase compared to the baseline scenario. Option 1 entails the participation of industry as part of self-regulatory initiatives. Option 2 would entail some

compliance costs based on the fact that the scope of some provisions would be broadened to OTTs and the fact that it includes some new costs, including e.g. in relation to unsolicited communications. At the same time, some savings would occur partially countering these additional costs. Under policy option 3, compliance costs are expected to decrease compared to the baseline scenario. Although there would also be some new costs, the options entail savings that are overall higher than the new costs. In particular, based on the exceptions introduced in relation to the consent rule, the number of businesses affected by the ePD is expected to decrease significantly. Furthermore, the policy option introduces some simplifications. The magnitude of the savings depends on the solution chosen in relation to the management of users' consent. The savings would be highest if consent would be solely managed via the browsers and lowest if consent would still be managed via individual websites. Under option 4, compliance costs are expected to increase due to the extension of the scope of the ePrivacy to OTTs, as well as explicitly prohibiting the practice of denying access to a website or an online service in case users do not provide consent to tracking. The prohibition of denying access to a website/service in case users do not consent to tracking will lead to an increase of IT costs for businesses. Businesses will need to amend their websites/services so that they are also available to the extent possible without the use of cookies. Under policy option 5, no compliance costs would ensue for businesses from the ePD anymore as it would be repealed entirely.

- **Administrative burden**: In the current situation, the main cost factors in relation in administrative burden relate to personal data breach notifications under Article 4 as well as the preparation for / dealing with audits by competent authorities. Option 1 does not affect these aspects. Options 2 and 3 both entail the deletion of the provision on personal data breach notifications. As this is one of the main cost factors (in some Member States applying to more companies than audits), a significant decrease of costs may be expected. Option 4 would also contribute to decreasing cost from administrative burden. Option 5 would remove the costs stemming from administrative burden in its entirety.

As a **fifth step**, for each of the ranges, we have indicated which "end of the range" is more likely to provide a picture of the actual, real-life value. The following assumptions were made based on expert judgment:

Table 5 –Qualitative assessment of the plausibility of the quantitative estimates

	Policy Option 1		Policy Option 2		Policy Option 3						Policy Option 4		Policy Option 5	
					Scenario 1		Scenario 2		Scenario 3					
Provision	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**
Number of citizens affected	X		X		X		X		X		X		X	
Number of businesses affected		X	X			X		X		X	X		X	
Compliance costs		X		X		X		X		X		X	X	

	Policy Option 1		Policy Option 2		Policy Option 3						Policy Option 4		Policy Option 5	
					Scenario 1		Scenario 2		Scenario 3					
Costs stemming from administrative burden	X			X		X	X		X		X		X	

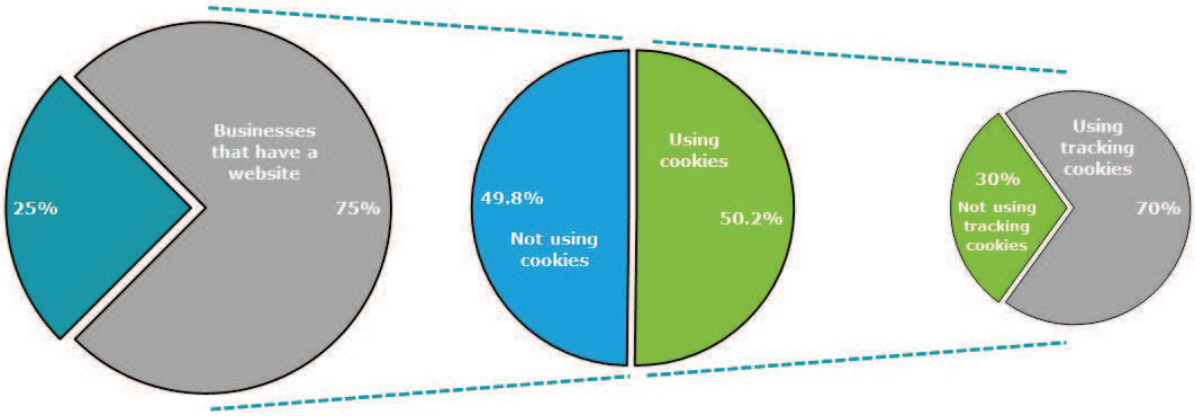
Source: Deloitte

As a **sixth and final step**, we have multiplied each of the selected percentages with the values estimated based on the "basic assumptions" (see previous section) per year (2016-2030), per Member State, and per size class of business. In the following sub-section, we provide the qualitative reasoning behind the quantitative assessments of the impacts of the policy options on businesses

1. Basic considerations concerning the share of websites potentially affected

Even before assessing the impacts of the policy options vis-à-vis the baseline scenario in both qualitative and quantitative terms, it is necessary to reflect what the basic population of businesses is on which the policy options can impact, as well as what the magnitude of the impacts on the number of businesses and their costs could be in theory. The basic population is visualised below.

Figure 1 – Basic population which the policy options can impact



Source: Deloitte

The figure above shows that the number of businesses that have a website (in this case e.g. 75%) is the basis for the estimates. Half of these websites (50.2%) use cookies, while the other half does not use cookies (49.8%). Only the former is relevant for the quantitative assessment of the policy options. Of the websites that use cookies, 70% use tracking cookies, while 30% do not use tracking cookies. The elements of the policy options relating to exceptions of the cookie consent rule under Art. 5(3) would, compared to the baseline situation, free those 30% of businesses from having to implement a cookie banner.

Possible technical solutions to collect the consent of the users

There are different potential technical solutions to facilitate users to diverge from their

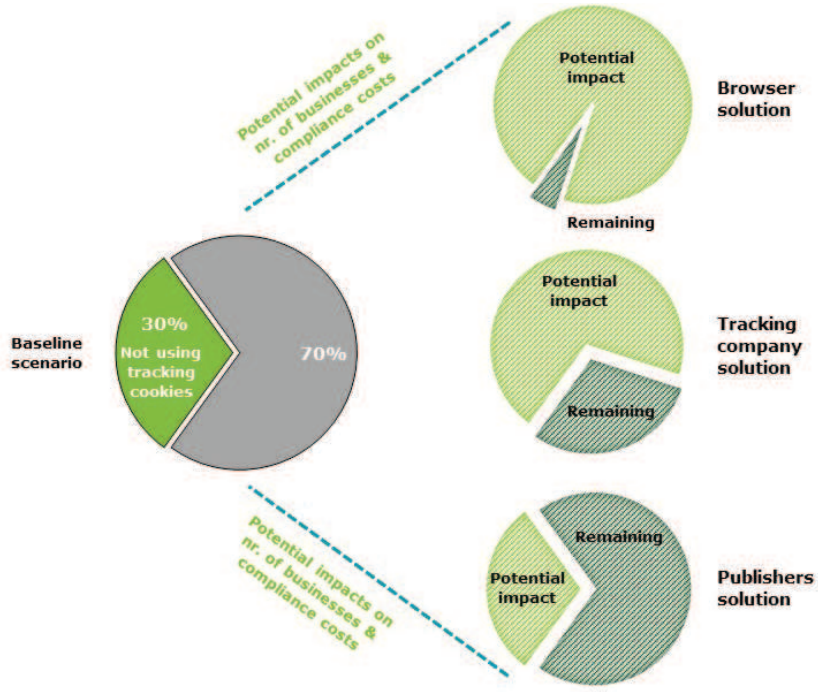
default setting for individual websites, all with different implications on costs. The following scenarios exist: (1) All communication runs centralised via the browsers; (2) The party placing the cookie is responsible for asking the consent; (3) Individual websites are responsible for asking the consent.

The impact of the policy options on the remaining 70% (see above) depends on the specific solution implemented e.g. under policy option 3:

- *Scenario 1 ("Browser solution"):* Assuming that the communication would exclusively run via the browsers, all the costs would lie with the browser providers (as reflected above). Websites on the other hand, would have no specific costs. Thus, in comparison to the current situation, websites would save the costs they incur now to implement the cookie banner. As this is considered the main cost associated for businesses, this would be a significant decrease.
- *Scenario 2 ("Tracking company solution"):* In this scenario, the costs would lie with the companies placing the data. It is expected that this would be slightly more expensive compared to solution 1, as a higher number of businesses would be concerned. Although most tracking cookies are placed by few main players, other smaller players will be affected as well. Furthermore, this solution would require the development of new practical and technical solutions to implement the option. Websites would have no specific costs. Thus, in comparison to the current situation, websites would save the costs they incur now to implement the cookie banner. As this is considered the main cost associated for businesses with the ePD, this would be a significant decrease.
- *Scenario 3 ("Publishers solution"):* In this case, there would be no significant changes for website operators, as they would in principle still employ cookie banners (or a similar technical solution).

This is depicted in the figure below.

Figure 2 – Potential magnitude of impacts of the scenarios under policy option 3



Source: Deloitte

It can be seen from the figure above that, in theory, it is expected that the "browser solution" would be able to free up most businesses from costs (the light green part of the pie chart at the top is largest) while costs are imposed on a small number of browser operators. In addition, a limited number of businesses would also incur "some" costs under this scenario. As part of the "tracking company solution", impacts on the number of businesses and compliance costs are also expected to be large, but less pronounced than under the "browser solution". The number of businesses that would still incur costs (i.e. "remain") would be a bit larger than under the "browser solution". Finally, the "publishers solution" is not expected to be *game changer* compared to the baseline situation as only the websites that do not use tracking cookies in the baseline scenario would be exempted under the ePD.

Key findings of the quantitative analysis: Average values over time

In this section, the policy options are compared against the baseline scenario.

As a first step, the main quantitative outcomes of the economic analysis are presented in the form of tables. This section will contain separate tables concerning:

- Average annual values;
- Absolute changes of the average annual value compared to the REFIT / baseline scenario; and
- Relative changes of the average annual value compared to the REFIT / baseline scenario.

This section contains the average values for the quantitative indicators:

- The number of businesses affected;
- Compliance costs, incl. average compliance costs per business; and

- Administrative burden, incl. average costs from admin. burden per business.

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

As a second step, the results are compared against the baseline scenario in the form of charts in order to be able to spot clearly the different impacts of the policy options compared to the baseline scenario.

A sub-section is devoted to each of the above quantitative indicators. Within each sub-section, different figures are provided in relation to: Micro-enterprises; SMEs; large enterprises; foreign controlled enterprises; and all businesses (i.e. the sum of the aforementioned).

In relation to policy option 3, only the "browser solution" has been visualised.

The number of citizens affected by the ePD under each policy option is not compared with the baseline scenario. The reason for this is that the policy options have no impact on the number of citizens affected – both are independent from each other. This means that, under each policy option, the number of citizens affected is equal to the baseline scenario.

Table 6 – Key figures of the quantitative assessments concerning businesses (absolute values)

Average annual value	REFIT	Today	Baseline scenario	Policy Option 1	Policy Option 2	Policy Option 3[146]			Policy Option 4	Policy Option 5
	(2002-2015)	(2016 snap shot)	(2016-2030)	(2016-2030)	(2016-2030)	(2016-2030)			(2016-2030)	(2016-2030)
						"Browser"	"Tracking companies"	"Publishers"		
Number of businesses affected (in million)	2.84	3.11	3.70	3.70	3.89	0.19	0.74	2.22	0.37	0.00
Micro-enterprises	2.53	2.78	3.31	3.31	3.48	0.17	0.663	1.99	0.33	0.00
SMEs	0.26	0.25	0.26	0.26	0.27	0.01	0.052	0.16	0.03	0.00
Large enterprises	0.01	0.01	0.01	0.01	0.01	0.00	0.002	0.01	0.001	0.00
Foreign controlled enterprises	0.05	0.06	0.12	0.12	0.13	0.01	0.024	0.07	0.01	0.00
Compliance costs (in million Euro)	1,861.7 €	1,505.7 €	1,355.4 €	1,423.15	1,558.7 €	406.6 €	542.152	1,287.6 €	1,287.6 €	0.0 €
Micro-enterprises	1,655.8 €	1,349.0 €	1,213.0 €	1,273.6 €	1,394.9 €	363.9 €	485.188	1,152.3 €	1,152.3 €	0.0 €
SMEs	169.8 €	122.2 €	97.0 €	101.9 €	111.6 €	29.1 €	38.808	92.2 €	92.2 €	0.0 €
Large enterprises	5.6 €	4.2 €	3.3 €	3.5 €	3.8 €	1.0 €	1.332	3.2 €	3.2 €	0.0 €
Foreign controlled enterprises	30.5 €	30.3 €	42.1 €	44.2 €	48.4 €	12.6 €	16.823	40.0 €	40.0 €	0.0 €
Average compliance cost per business (in Euro)	658.4 €	484.5 €	373.5 €	392.2 €	409.1 €	2,240.9 €	746.978	591.4 €	3,548.1 €	0.0 €
Administrative burden (in million Euro)	0.28 €	0.23 €	0.23 €	0.23 €	0.21 €	0.208 €	0.226 €	0.23 €	0.22 €	0.00 €
Micro-enterprises	0.23 €	0.19 €	0.18 €	0.18 €	0.16 €	0.163 €	0.178 €	0.18 €	0.18 €	0.00 €
SMEs	0.03 €	0.03 €	0.03 €	0.03 €	0.03 €	0.031 €	0.033 €	0.03 €	0.03 €	0.00 €
Large enterprises	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €	0.002 €	0.002 €	0.00 €	0.00 €	0.00 €
Foreign controlled enterprises	0.02 €	0.01 €	0.01 €	0.01 €	0.01 €	0.013 €	0.014 €	0.01 €	0.01 €	0.00 €
Average costs from admin. burden per business (in Euro)	48.9 €	36.0 €	27.8 €	28.0 €	23.8 €	499.5 €	135.982 €	45.33 €	269.2 €	0.0 €

Source: Deloitte

[146] As part of this model, it was not possible to estimate reasonable average compliance costs and costs from administrative burden for businesses for the "browser" and the "tracking companies solution" of policy option 3. The reason for this is that the average costs are calculated on the basis of all businesses affected, i.e. also those that would incur higher costs than others and vice versa. As part of these two solutions, however, a very small share of businesses would have to bear the largest share of costs (i.e. browser operators and tracking companies) while the costs would be significantly lower for others. Therefore, it is not appropriate to indicate an "average amount per business" as this would return misleading estimates.

Table 7 – Key figures of the quantitative assessments concerning businesses (absolute changes)

Absolute changes of the average annual value compared to the REFIT / baseline scenario	REFIT	Today	Baseline scenario	Policy Option 1	Policy Option 2	Policy Option 3			Policy Option 4	Policy Option 5
	(2002-2015)	(2016 snap shot)	(2016-2030)	(2016-2030)	(2016-2030)	(2016-2030)			(2016-2030)	(2016-2030)
						"Browser"	"Tracking companies"	"Publishers"		
Number of businesses affected (in million)	n/a	n/a	0.86	0.00	0.19	-3.52	-2.96	-1.48	-3.33	-3.70
Micro-enterprises	n/a	n/a	0.78	0.00	0.17	-3.15	-2.65	-1.33	-2.98	-3.31
SMEs	n/a	n/a	0.00	0.00	0.01	-0.25	-0.21	-0.10	-0.24	-0.26
Large enterprises	n/a	n/a	0.00	0.00	0.00	-0.01	-0.01	0.00	-0.01	-0.01
Foreign controlled enterprises	n/a	n/a	0.07	0.00	0.01	-0.12	-0.10	-0.05	-0.11	-0.12
Compliance costs (in million Euro)	n/a	n/a	-506.3 €	67.8 €	203.3 €	-948.8 €	-813.2 €	-67.8 €	-67.8 €	-1,355.4 €
Micro-enterprises	n/a	n/a	-442.8 €	60.6 €	181.9 €	-849.1 €	-727.8 €	-60.6 €	-60.6 €	-1,213.0 €
SMEs	n/a	n/a	-72.8 €	4.9 €	14.6 €	-67.9 €	-58.2 €	-4.9 €	-4.9 €	-97.0 €
Large enterprises	n/a	n/a	-2.3 €	0.2 €	0.5 €	-2.3 €	-2.0 €	-0.2 €	-0.2 €	-3.3 €
Foreign controlled enterprises	n/a	n/a	11.6 €	2.1 €	6.3 €	-29.4 €	-25.2 €	-2.1 €	-2.1 €	-42.1 €
Average compliance cost per business (in Euro)	n/a	n/a	-284.9 €	18.7 €	35.6 €	1,867.4 €	373.5 €	217.9 €	3,174.7 €	-373.5 €
Administrative burden (in million Euro)	n/a	n/a	-0.04 €	0.002 €	-0.02 €	-0.023 €	-0.005 €	-0.005 €	-0.007 €	-0.23 €
Micro-enterprises	n/a	n/a	-0.05 €	0.002 €	-0.02 €	-0.018 €	-0.003 €	-0.004 €	-0.006 €	-0.18 €
SMEs	n/	n/	0.01 €	0.000 €	0.00 €	-0.003 €	-0.001 €	-0.001 €	-0.001 €	-0.03 €
Large enterprises	n/a	n/a	0.00 €	0.000 €	0.00 €	0.000 €	0.000 €	0.000 €	0.000 €	0.00 €
Foreign controlled enterprises	n/a	n/a	0.00 €	0.000 €	0.00 €	-0.001 €	0.000 €	0.000 €	0.000 €	-0.01 €
Average costs from admin. burden per business (in Euro)	n/a	n/a	-21.2 €	0.278 €	-4.0 €	471.8 €	108.2 €	17.6 €	241.4 €	-27.8 €

Source: Deloitte

Table 8 – Key figures of the quantitative assessments concerning businesses (relative changes)

Relative changes of the average annual value compared to the REFIT / baseline scenario	REFIT	Today	Baseline scenario	Policy Option 1	Policy Option 2	Policy Option 3			Policy Option 4	Policy Option 5
	(2002-2015)	(2016 snap shot)	(2016-2030)	(2016-2030)	(2016-2030)	(2016-2030)			(2016-2030)	(2016-2030)
						"Browser"	"Tracking companies"	"Publishers"		
Number of businesses affected (in million)	n/a	n/a	30.2%	0.0%	5.0%	-95.0%	-80.0%	-40.0%	-90.0%	-100.0%

Relative changes of the average annual value compared to the REFIT / baseline scenario	REFIT	Today	Baseline scenario	Policy Option 1	Policy Option 2	Policy Option 3			Policy Option 4	Policy Option 5
	(2002-2015)	(2016 snap shot)	(2016-2030)	(2016-2030)	(2016-2030)	(2016-2030)			(2016-2030)	(2016-2030)
						"Browser"	"Tracking companies"	"Publishers"		
Micro-enterprises	n/a	n/a	30.9%	0.0%	5.0%	-95.0%	-80.0%	-40.0%	-90.0%	-100.0%
SMEs	n/a	n/a	1.6%	0.0%	5.0%	-95.0%	-80.1%	-39.8%	-90.0%	-100.0%
Large enterprises	n/a	n/a	0.0%	0.0%	0.0%	-100.0%	-77.8%	-44.4%	-88.9%	-100.0%
Foreign controlled enterprises	n/a	n/a	157.4%	0.0%	5.0%	-95.0%	-80.2%	-40.5%	-90.1%	-100.0%
Compliance costs (in million Euro)	n/a	n/a	-27.2%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
Micro-enterprises	n/a	n/a	-26.7%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
SMEs	n/a	n/a	-42.9%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
Large enterprises	n/a	n/a	-40.9%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
Foreign controlled enterprises	n/a	n/a	38.0%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
Average compliance cost per business (in Euro)	n/a	n/a	-43.3%	5.0%	9.5%	500.0%	100.0%	58.3%	850.0%	-100.0%
Administrative burden (in million Euro)	n/a	n/a	-16.0%	0.9%	-10.0%	-10.0%	-2.2%	-2.2%	-3.0%	-100.0%
Micro-enterprises	n/a	n/a	-21.3%	1.1%	-9.9%	-9.9%	-1.7%	-2.2%	-3.3%	-100.0%
SMEs	n/	n/	25.9%	0.0%	-8.8%	-8.8%	-2.9%	-2.9%	-2.9%	-100.0%
Large enterprises	n/a	n/a	-33.3%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	-100.0%
Foreign controlled enterprises	n/a	n/a	-6.7%	0.0%	-7.1%	-7.1%	0.0%	0.0%	0.0%	-100.0%
Average costs from admin. burden per business (in Euro)	n/a	n/a	-43.3%	1.0%	-14.3%	1700.0%	390.0%	63.3%	870.0%	-100.0%

Source: Deloitte

ANNEX 9: COVERAGE OF OTTS WITHIN THE SCOPE OF NATIONAL IMPLEMENTING LEGISLATION

The interpretation and implementation of the scope varies across Member States. Indeed, some Member States have extended the ePD provisions to OTT services. Spain, UK, Austria, France, Estonia, Croatia, Finland, Denmark, Latvia, Norway, The Netherlands, Germany and Spain consider VoIP with access to telephone number an electronic communications service[147]. To the contrary, peer-peer VoIP does not constitute the said service by the countries previously mentioned. In the Czech Republic VoIP communication is considered an electronic communications service solely in cases where the communication is secured by a third party (external) provider within the scope of such provider's business. The German competent authority explained that they consider the scope of the ePD to be unclear in this respect[148].

Country	OTTs covered	OTTs not covered	Case-by-case	No information/ unclear
Austria	X			
Belgium				X
Bulgaria	X			
Croatia				X
Cyprus				X
Czech Republic		X		
Denmark				X
Estonia		X		
Finland				X
France	X			
Germany			X	
Greece	X			
Hungary				X
Ireland		X		
Italy			X	
Latvia	X			
Lithuania				X
Luxembourg		X		
Malta				X
Netherlands		X		
Poland		X		
Portugal		X		
Romania		X		

[147] Swedish Post and Telecom Agency (PTS), "Which services and networks are subject to the Electronic Communications Act", guidance, 11 March 2009, Stockholm, p. 16.
[148] *Source: Deloitte (SMART 2016/0080).*

Country	OTTs covered	OTTs not covered	Case-by-case	No information/ unclear
Slovakia		X		
Slovenia	X			
Spain	X			
Sweden				X
UK				X
Overall	7	9	2	10

Source: Deloitte (SMART 2016/0080) – Transposition check

ANNEX 10: OPT-IN AND OPT-OUT REGIMES PER MEMBER STATE

The table below further illustrates the wide diversity of regimes on unsolicited communications calls (with human intervention) and the fragmentation of the rules in the EU. The table shows that in relation to fixed-line phones, 24% of EU businesses currently are governed by an opt-in regime while the share is 52% in relation to mobile phones[149]. By contrast, 88% of EU businesses are currently governed by an opt-out regime in relation fixed-line phones while 61% are governed by an opt-in regime.[150]

Member States	Number of businesses	Fixed-line phones		Mobile phones	
		Opt-in	Opt-out	Opt-in	Opt-out
Austria	321,661	X		X	
Belgium	593,421		X	X	
Bulgaria	319,856	X		X	
Croatia	147,337		X		X
Cyprus	46,938	X		X	
Czech Republic	995,754		X		X
Denmark	212,740	X[1]	X[2]	X[1]	X[2]
Estonia	64,040		X		X
Finland	229,248		X		X
France	3,188,138		X	X	
Germany	2,193,135	X[1]	X[3]	X[1]	X[3]
Greece	700,166		X		X
Hungary	514,537	X		X	
Ireland	146,741		X	X	
Italy	3,715,164		X		X
Latvia	100,491	X		X	
Lithuania	174,611	X		X	
Luxembourg	31,385	X		X	
Malta	26,193		X		X
Netherlands	1,054,562		X		X
Poland	1,549,326		X		X
Portugal	781,823	X		X	
Romania	455,852	X		X	
Slovakia	400,683	X[1]	X[3]	X[1]	X[3]
Slovenia	130,088		X		X

[149] The sum of the percentages is higher than 100%, as traders is some countries (Denmark, Germany, Slovakia) are subject to both opt-in and opt-out, depending on the type of addressee (e.g., natural or legal persons).

[150] *Source: European Commission, tabulation by Deloitte (SMART 2016/0080) [1]For 'consumers'; [2]For 'businesses'; [3]For 'other market players'. Statistical data from taken from Eurostat (most recent data from 2014). Some exceptions apply to the opt-in consent rule for consumers in Denmark.*

Member States	Number of businesses	Fixed-line phones		Mobile phones	
		Opt-in	Opt-out	Opt-in	Opt-out
Spain	2,377,191		X	X	
Sweden	673,218		X		X
United Kingdom	1,841,715		X		X
		12	19	16	15
Number / share of businesses affected	22,986,014	5,553,712	20,238,860	11,859,203	13,933,369
		24%	88%	52%	61%

ANNEX 11: TABLE OF COMPETENT AUTHORITIES

The enforcement of the ePD provisions at national level is entrusted to a "*competent national authority*" (Article 15a of the ePD), without further defining that authority or body. This has led to a fragmented situation in the EU and within Member States. Member States have allocated the competence to DPAs, telecom NRAs, to another type of body (e.g. consumer protection bodies) or to several different bodies within the same country.

The table below shows that not only competence for the ePD is scattered over several authorities, but that competence can even be scattered per article. For Article 13, in 11 Member States the DPA has sole competence, in 1 Member States the consumer agency has sole competence and in 4 Member States the NRA and DPA share competence. In the remaining Member States other combinations of authorities, up to five different ones, have competence on Article 13. Article 13 stands as an example for the distribution of competences for the other ePD articles.

The current situation in which several authorities can be in charge of the ePD and several authorities can be in charge of one article causes several risks:

- The risk of having several interpretations of ePD provisions within one Member State. The different competent authorities may have different views and use different enforcement strategies;

- The risk of duplication of enforcement powers of the same article, which is detrimental for consumers. It may be difficult to single out the enforcers to complain to and the risk exists they are send back and forth between authorities.

Above is multiplied when you take it to a European level.

Moreover, there is no recognised EU group to gather together all authorities responsible for the enforcement of the ePD: indeed, DPAs meet through the Article 29 Working Party, NRAs through BEREC. Some consumer bodies meet through the Consumer Protection Cooperation (CPC) network.

Country	Article 5	Articles 6 & 9	Article 13
Austria	NRA Telecom office	NRA Telecom office	NRA Telecom office DPA
Belgium	NRA Ombudsman for telecoms Regional supervisory authorities for the media sector DPA	NRA Ombudsman for telecoms Regional supervisory authorities for the media sector	NRA Ombudsman for telecoms Regional supervisory authorities for the media sector Ministry for Economy DPA

Country	Article 5	Articles 6 & 9	Article 13
Bulgaria	NRA DPA Commission for Consumer Protection	NRA Commission for Consumer Protection	NRA Commission for Consumer Protection DPA
Croatia	NRA DPA	NRA DPA	NRA DPA Ministry for Economic Affairs Ministry of Finance
Cyprus	NRA DPA	NRA DPA	NRA DPA
Czech Republic	DPA	DPA	DPA
Denmark	DPA	The Telecommunications Complaints Board	Competition and Consumer Authority Consumer Ombudsman
Estonia	NRA	NRA	DPA
Finland	NRA	DPA	DPA
France	DPA NRA	DPA NRA	DPA NRA Ministry for Economic Affairs
Germany	DPA NRA Data Protection Commissioners of the German Lands (for art. 5.3)	DPA NRA	DPA NRA
Greece	DPA NRA	DPA NRA	DPA NRA
Hungary	DPA NRA (except 5(3))	DPA NRA	NRA DPA Consumer Protection Inspectorates / National Authority
Ireland	DPA	DPA NRA	DPA
Italy	DPA	DPA	DPA
Latvia	Ministry of Transport NRA DPA - 5(3)	Ministry of Transport DPA	Ministry of Transport DPA Consumer Protection Authority

Country	Article 5	Articles 6 & 9	Article 13
Lituania	DPA	DPA	DPA
Luxembourg	DPA	DPA	DPA
Malta	DPA	DPA	DPA
The Netherlands	Consumer Protection Authority DPA NRA (5(1))	DPA NRA	Consumer Protection Authority DPA
Poland	DPA NRA	DPA NRA	DPA Office of Competition and Consumer Protection NRA
Portugal	DPA NRA (5(1))	DPA	DPA
Romania	DPA	DPA	DPA
Slovakia	Ministry of Transport NRA Ministry of Finance (5(3))	Ministry of Transport NRA	Ministry of Transport NRA
Slovenia	NRA	NRA DPA	NRA Market Inspectorate
Spain	DPA	DPA	DPA
Sweden	NRA	NRA	Consumer Agency
UK	NRA DPA	NRA DPA	NRA DPA Financial Authority

Source: on the basis of European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector (SMART 2016/0080).

ANNEX 12: MAPPING OF THE POLICY OPTIONS

I.Table: Summary overview of Policy Options

	Policy Option 1 Soft law measures	**Policy Option 2** Limited reinforcement of privacy and harmonisation	**Policy Option 3** Measured reinforcement of privacy and harmonisation	**Policy Option 4** Far-reaching reinforcement of privacy and harmonisation	**Policy Option 5** Repeal of the ePD
Objective 1 - *Ensuring effective confidentiality of electronic communications*	1. **Increased use of interpretative communications**. 2. **Support EU-wide self-regulatory initiatives** 3. **Specify privacy by design requirements of terminal electronic equipment through EU standards**. 4. **Research and awareness-raising activities**.	1. **Extension of the scope** of the ePD to OTTs providing communications functions, such as webmail, Internet messaging, VoIP. 2. Clarify that the ePD applies to communication running over **publicly available communications networks**, such as in particular commercial Wi-Fi networks in stores, hospitals, airports, etc. 3. Specify that confidentiality rules, including of terminal equipment, apply to any machine that is connected to the network (including M2M communications, such as for example, a refrigerator	1. Measures 1 to 3 of Option 2. 2. The new instrument would propose a technology neutral definition of electronic communications, encompassing all the additional elements under **Option 2** (1, 2 and 3). 3. On the subject of confidentiality of terminal equipment and tracking of online behaviour the envisaged	1. All the measures under No 1, 2, 3 and 4 of **Option 3**. 2. Explicitly **prohibit the practice of denying access to a website** or an **online service** in case users do not provide consent to tracking (so-called cookie-wall).	1. The GDPR provides for reinforced rights of individuals and the obligations of data controllers, which are in keeping up with the challenges of the digital age. The **consent rule** under the GDPR has been in particular **substantially strengthened** with a view to ensure that it is freely-given. The GDPR addressed the issue of

		connected to a grocery store web site).	proposal would reformulate and simplify the "cookie" centred approach in favour of a technology neutral approach applying to all forms of tracking of (or other interference with) users' online behaviour, irrespective of the technique employed. The proposal would clarify that **consent can be given by means of the appropriate settings** of a browser or other application. The proposal would require certain software providers that support a terminal equipment basic functions (e.g. Internet browsers and OSs) to provide their products with privacy friendly		unbalance of economic power between the controller and the processor, requesting that this aspect be taken into account in the assessment of the validity of consent. 2. The GDPR would guarantee more effective enforcement in view of the reinforced powers conferred on data protection authorities.

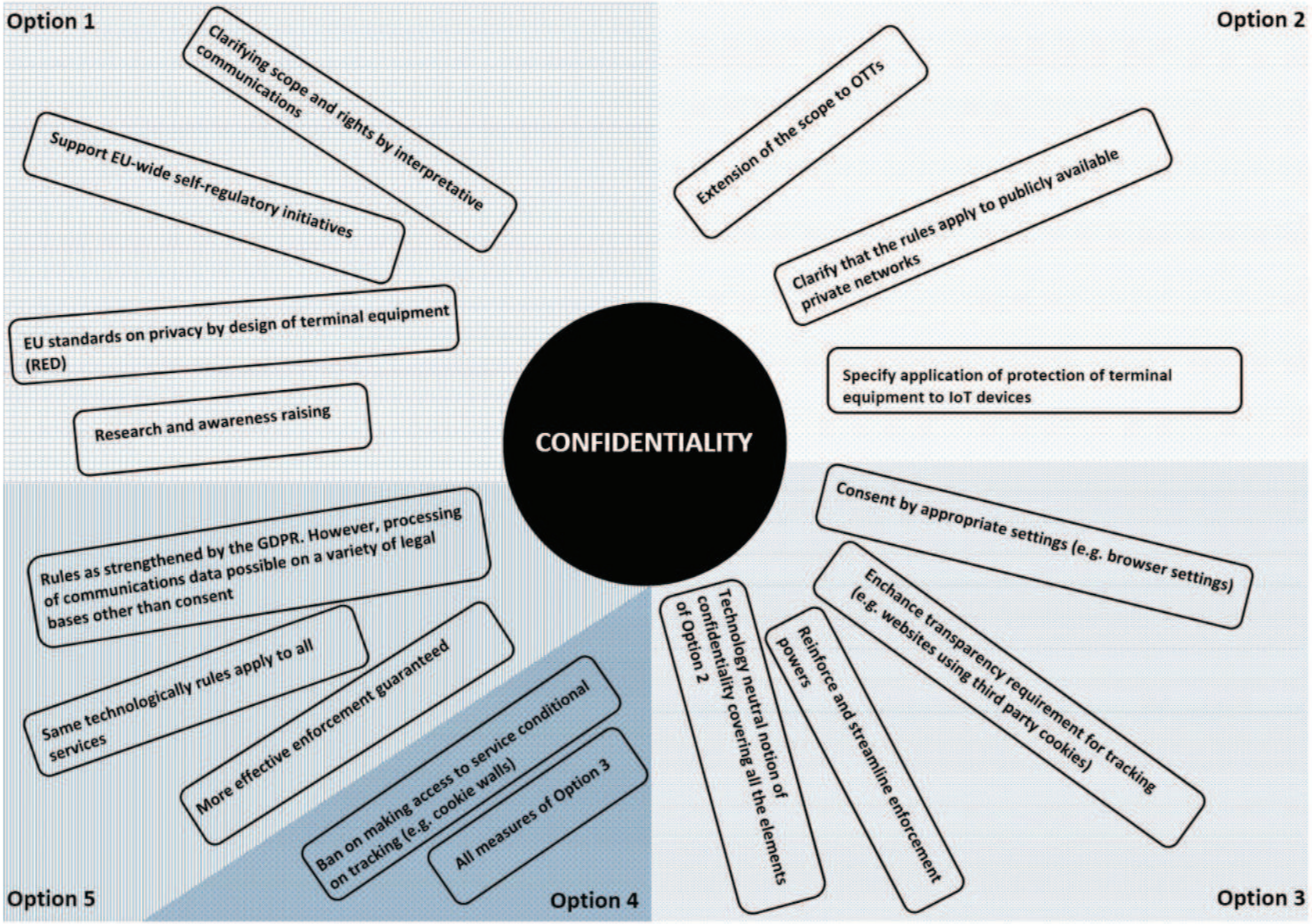
			settings as a means to provide consent and to reinforce user's control over online tracking and the over the flow of data from and into their terminal equipment. 4. Impose **enhanced transparency requirements** on entities processing communications data (e.g. websites, mobile apps and publicly available Wi-Fi private networks). 5. **Reinforce and streamline enforcement powers**: The new instrument would entrust the application and enforcement of the provisions of the ePrivacy instrument to the same independent supervisory authorities		

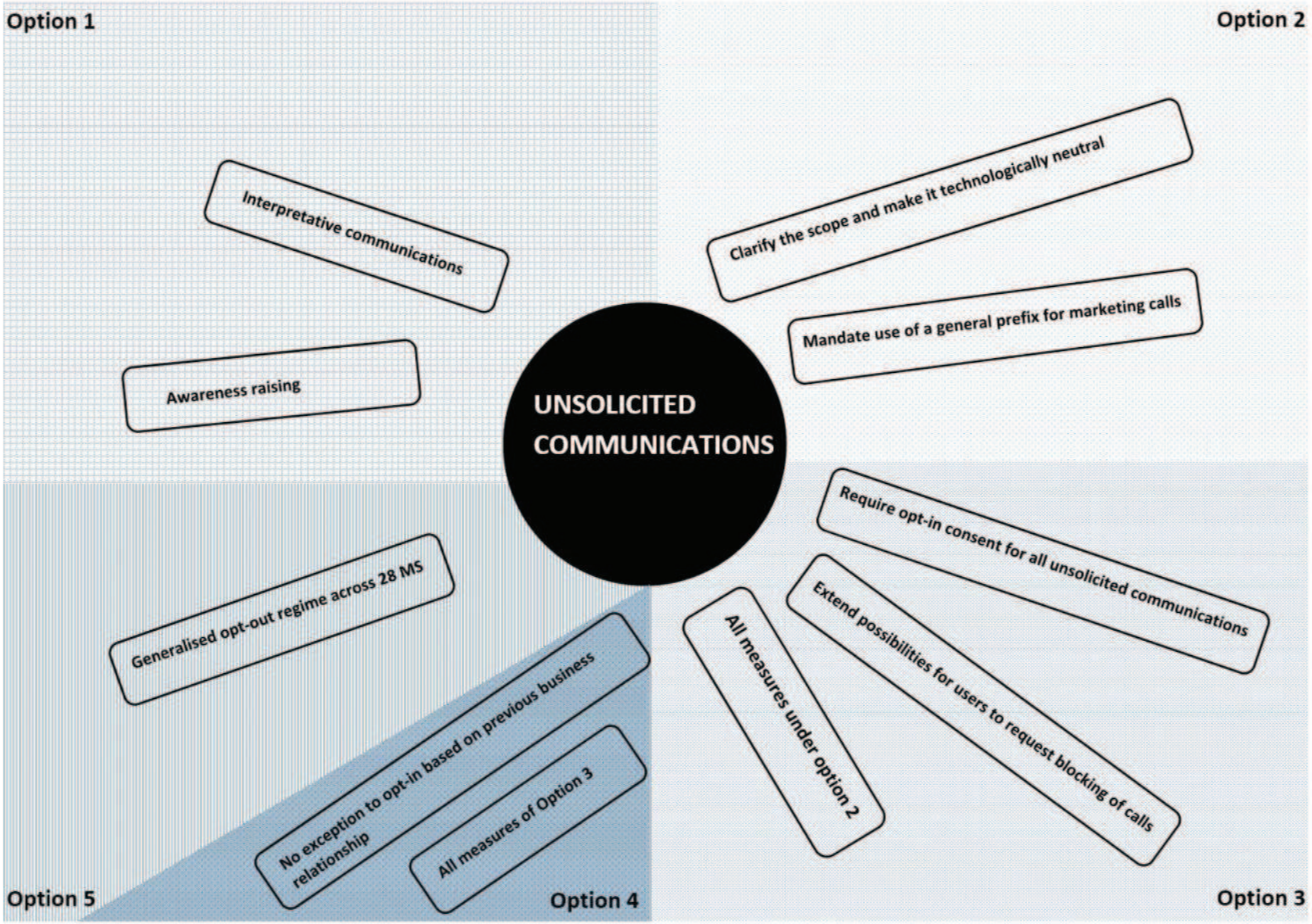
			appointed under the GDPR.		
Objective 2 - *Ensuring effective protection against unsolicited commercial communications*	1. **Interpretative communications**, clarifying the interpretation of unclear or ambiguous concepts. 2. **Awareness-raising initiatives** instructing citizens on how to defend themselves, how to seek redress from national supervisory authorities.	4. **Clarify the scope of the provision on unsolicited communications and make it technologically neutral**: clarify that it applies to any form of unsolicited electronic communication, irrespective of the technological means used (e.g. wallpapers, mailboxes, etc.). 5. **Require for marketing calls the use of a special prefix** distinguishing direct marketing calls from other calls.	6. All the measures from 4 to 5 under **Option 2**. 7. Require **opt-in consent for all types of unsolicited communications covered by the current rules**. 8. Clarify the provision on **presentation of calling line identification** to include the right of users to reject calls from specific numbers (or categories of numbers).	1. All the measures under No 6 and 7 of **Option 3**. **2.** Under this option, the Commission would **repeal** the provision allowing direct marketers to send communications to subscribers and users when they have received their contact details in the context of a **previous business relationship**	**3.** Unsolicited communications would be essentially regulated under a general **opt-out** regime across 28 MS
Objective 3 - *Enhancing harmonisation and simplifying/updating the legal framework*	3. Issue **interpretative communications** to promote an application of the current rules,	6. **Reinforce cooperation obligations** among the competent authorities, including for cross-border enforcement. Under this option, the Commission	8. Propose changes aimed at **clarifying and minimising the margin of manoeuvre of certain provisions**	13. Measures under No 8, 9, 10, 11 and 12 of Option 3. 14. Introduce	1. All providers of electronic communications will be subject to the **same rules** without

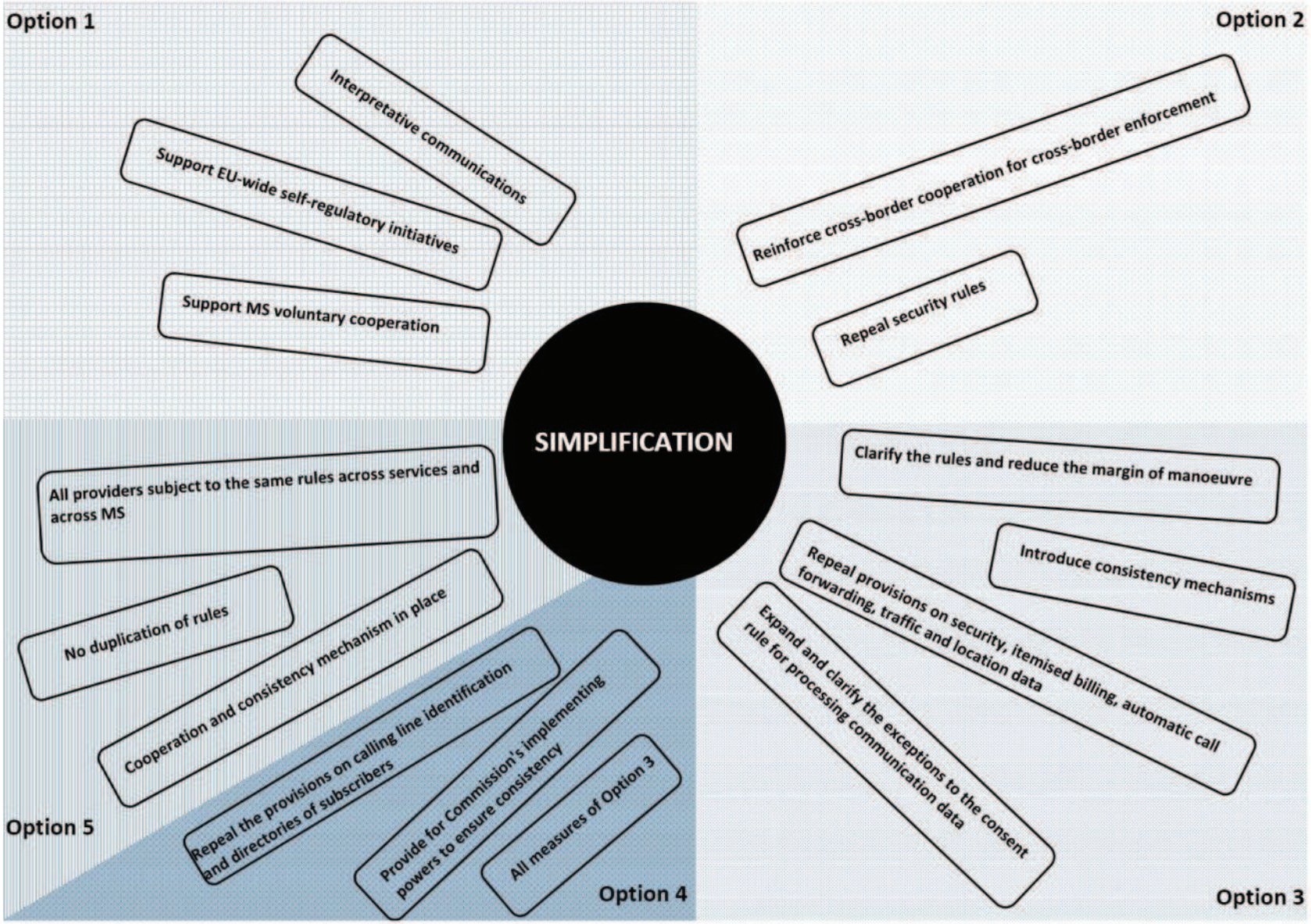
	which is business friendly, while preserving the essence of the protection of confidentiality of communications 4. Work closely with **industry** in order to encourage the adoption of **common best practices**. 5. **Support MS cooperation** to improve enforcement in cross-border cases as well as harmonised interpretation by organising meetings and workshops with authorities	would propose an obligation for supervisory authorities to cooperate with other supervisory authorities and provide each other with relevant information and mutual assistance. 7. **Repeal of the security rules** leaving the matter to be regulated by the corresponding rules in the Telecom Framework and the GDPR. The sole exception would be the rules on notification of users of security risks, which is indeed not covered by the latter instruments.	identified by stakeholders as a source of confusion and legal uncertainty. This will be achieved e.g. by regulating applicable law and territorial scope, clarifying the scope of the provisions concerning confidentiality of communications, the scope and requirements concerning confidentiality of terminal equipment and the rules on unsolicited advertising. 9. Extend the application of the consistency mechanism established under the GDPR to the ePrivacy instrument. 10. Repeal provisions on **security** and the provisions on	Commission's implementing powers for deciding on the correct application of the ePrivacy rules. order to ensure correct and consistent application of the EU law.	discrimination based on the technology used. 2. There would be no duplication of rules in the security area and all the ePD provisions related to specific issues in the electronic communications sector (e.g. directories of subscribers) would be dealt with on the basis of the general data protection rules.

			itemised billing. 11. Repeal the provisions on **traffic data and location data.** The processing of traffic and location data will be regulated under the general provision of confidentiality of communications data. 12. Specify that service providers can only process communications data with the consent of the users. Providing for **additional/broadened exceptions** to the consent and enhanced transparency rules for specific purposes which give rise to little or no privacy risks.		

II.Visualisation of the various elements of the policy options in relation to the specific objectives


Option 1
Clarifying scope and rights by interpretative communications
Support EU-wide self-regulatory initiatives
EU standards on privacy by design of terminal equipment (RED)
Research and awareness raising
Option 2
Extension of the scope to OTTs
Clarify that the rules apply to publicly available private networks
Specify application of protection of terminal equipment to IoT devices
CONFIDENTIALITY
Option 5
Rules as strengthened by the GDPR. However, processing of communications data possible on a variety of legal bases other than consent
Same technologically rules apply to all services
More effective enforcement guaranteed
Option 4
Ban on making access to service conditional on tracking (e.g. cookie walls)
All measures of Option 3
Option 3
Consent by appropriate settings (e.g. browser settings)
Enchance transparency requirement for tracking (e.g. websites using third party cookies)
Reinforce and streamline enforcement powers
Technology neutral notion of confidentiality covering all the elements of Option 2


Option 1
Option 2
Interpretative communications
Clarify the scope and make it technologically neutral
Mandate use of a general prefix for marketing calls
Awareness raising
UNSOLICITED COMMUNICATIONS
Require opt-in consent for all unsolicited communications
Extend possibilities for users to request blocking of calls
All measures under option 2
Generalised opt-out regime across 28 MS
No exception to opt-in based on previous business relationship
All measures of Option 3
Option 5
Option 4
Option 3


Option 1
Interpretative communications
Support EU-wide self-regulatory initiatives
Support MS voluntary cooperation
Option 2
Reinforce cross-border cooperation for cross-border enforcement
Repeal security rules
SIMPLIFICATION
All providers subject to the same rules across services and across MS
No duplication of rules
Cooperation and consistency mechanism in place
Repeal the provisions on calling line identification and directories of subscribers
Provide for Commission's implementing powers to ensure consistency
All measures of Option 3
Option 5
Option 4
Clarify the rules and reduce the margin of manoeuvre
Introduce consistency mechanisms
Repeal provisions on security, itemised billing, automatic call forwarding, traffic and location data
Expand and clarify the exceptions to the consent rule for processing communication data
Option 3

ANNEX 13: DETAILED COMPARISON OF POLICY OPTIONS

The following table reflects the assessment of the **effectiveness** policy options as per Section 6.1.1 of the impact assessment report.

Table 2: **Comparison of options in terms of effectiveness**

	Objective 1 - *Confidentiality*	**Objective 2 –** *Unsolicited communications*	**Objective 3 –** *Harmonisation/simplification*	**Total**
Option 0 -- *Baseline*	0	0	0	0
Option 1 – *Soft law*	✓	≈	✓	✓✓
Option 2 – *Limited reinforcement/harmonisation*	✓✓	✓	≈	✓✓✓
Option 3 – *Measured reinforcement/harmonisation*	✓✓	✓✓	✓✓	✓✓✓✓✓✓
Option 4 – *Far-reaching reinforcement/harmonisation*	✓✓✓	✓✓	✓✓✓	✓✓✓✓✓✓✓✓✓
Option 5 – *Repeal*	××	×	✓✓✓	≈

Effectiveness of the various policy options vis-à-vis the specific objectives, ✓✓✓(Strong and positive– ✓✓ (Moderate and positive) – ✓ (Weak and positive) - ×××(Strong and negative) – ××(Moderate and negative) – × (Weak and negative) – ≈ marginal or neutral - ? uncertain; n.a. not applicable. 0 no impact

The following table reflects the assessment of the **efficiency** of the policy options as per Section 6.1.2 of the impact assessment report.

Table 3: Comparison of options in terms of efficiency

	Compliance cost (incl. for public administration)	**Administrative burden**	**Opportunity Cost**	**Total**
Option 0 – *Baseline*	0	0	0	0
Option 1 – *Soft law*	×	n.a.	n.a.	×
Option 2 – *Limited reinforcement/harmonisation*	×	≈	××	×××
Option 3 – *Measured reinforcement/harmonisation*	✓✓✓	≈	××	✓

Option 4 – *Far-reaching reinforcement/harmonisation*	××	≈	×××	×××××
Option 5 – *Repeal*	n.a.	n.a.	✓✓✓	✓✓✓

Impact on cost/efficiency of the various policy options, ✓✓✓(Strong and positive– ✓✓ (Moderate and positive) – ✓ (Weak and positive) - ×××(Strong and negative) – ××(Moderate and negative) – × (Weak and negative) – ≈ marginal or neutral - ? uncertain; n.a. not applicable. 0 no impact

---

The following table reflects the assessment of the **coherence** of policy options as per Section 6.1.3 of the impact assessment report.

Table 4: Comparison of options in terms of coherence

	Internal coherence	**Telecom framework**	**GDPR**	**RED**	**Total**
Option 0 -- *Baseline*	0	0	×	**0**	×
Option 1 – *Soft law*	×	×	×	**0**	×××
Option 2 – *Limited reinforcement/ harmonisation*	✓	✓	✓	**0**	✓✓✓
Option 3 – *Measured reinforcement/ harmonisation*	✓✓	✓	✓	≈	✓✓✓✓
Option 4 – *Far-reaching reinforcement/ harmonisation*	✓	✓	✓	≈	✓✓✓
Option 5 – *Repeal*	×	✓	✓	**0**	✓

Impact on coherence, ✓✓✓(Strong and positive– ✓✓ (Moderate and positive) – ✓ (Weak and positive) - ×××(Strong and negative) – ××(Moderate and negative) – × (Weak and negative) – ≈ marginal or neutral - ? uncertain; n.a. not applicable. 0 no impact

2. Comparison of options with respect to their impact on different stakeholders

- Option 1 to 4 will benefit **Citizens** (both individuals and legal persons) in increasing magnitude due to the reinforcement of the protection of their privacy. **Option 1** will have a slightly positive effect, through the dissemination of guidance, best practices, standardisation and awareness-raising initiatives. **Option 2** will have a positive effect, thanks in particular to the extension of the scope of the protection. **Option 3** will have greater positive effects thanks to the introduction of mandatory centralised privacy settings. **Option 4** will further increase the level of protection, but may indirectly penalise citizens by excessively limiting OBA based offers. **Option 5** would remove the specific protection of privacy and confidentiality in the electronic communications secor and in this respect may penalise citizens. **Option 3** is the best option for citizens.

- **Businesses:** the following main cateogories of different undertakings would be affected by the new rules in the following way:

  - ✓ **ECS providers**: **Option 1** does not affect ECS providers much. ECS providers would benefit from the level playing field introduced by **Options 2, 3** and **4**. **Option 5** would benefit ECS providers the most, as it would simplify the rules applicable to them and eliminate the specific restrictions concerning traffic and location data. **Option 5** is the best option for ECS providers. Between **Option 2** and **3**, ECS providers would prefer **Option 3** as it would introduce elements of flexibility compared to the present regime.

  - ✓ **OTTs**: **Option 1** and **5** are the most favourable solutions for them, with possibly a preference for Option 1 given that this option would maintain their regulatory advantage over ECS providers. **Option 2, 3** and **4** would significantly affect OTTs as they will have to comply with the ePrivacy rules. Between these, **Option 3** is to be preferred due to the greater flexibility, whereas **Option 4** is the most restrictive.

  - ✓ **Website operators** and **online advertisers**: **Options 1** and **2** would not change anything for these operators. **Option 3** would present some advantages in terms of cost reduction and some disadvantages relating to the binding browser privacy settings greater transparency of tracking. **Option 4** would seriously affect them by banning the cookie wall. **Option 5** is the best option for them as it would basically imply removal of the current rules.

  - ✓ **Providers of browsers, operating systems and app stores** are only affected by **Option 3** in relation to the obligation to provide for general privacy settings. However, the related cost is not expected to be excessively high, considering that the few operators concerned already have developed some solutions in this direction.

  - ✓ **Direct marketers** would not be significantly affected by **Option 1**. They would be affected in increasing magnitude by **Option 2, 3** and **4**. **Option 5** is their most favourite option, as it would remove at least in part the restrictions regarding unsolicited marketing.

  - ✓ **SMEs** who are OTTs would be affected significantly by **Option 2**, **3**, and **4** given the extension of the scope. Compared to large businesses, they would feel in proportion more the burden of the new ePrivacy rules. However, some flexibility and simplification mechanisms included in Option would significantly reduce such burden.

- **Competent authorities**: **Option 3** and **4** will have significant effects on national authorities. **Option 3** would entail some reorganisation costs for those authorities that are currently not equipped with appropriate powers and adequate resources for exercising supervision.

- The **Commission** will have to bear some costs relating to the various soft-law initiatives in **Option 1**. The costs for the Commission are low in **Option 2** and **3** and essentially coinciding with the conduct of the legislative process. In addition, the Commission would have to bear some variable running costs for the implementing measures in **Option 4**.

The above analysis shows that **Option 3** is the best option for citizens, while **Option 5** is the worst. By contrast, **Option 5** is the best option for businesses overall (the second best option for OTTs) and **Option 4** the worst. **Option 4** and **5** being excluded as extreme solutions, **Option 3** is overall a preferable solution to Option **2** for both citizens and businesses (except

some browsers providers). For MS authorities, **Option 3** presents non-insignificant reorganizational costs.

Table 5 – Comparison of options in terms of impact on stakeholders

Impacts	Option 0	Option 1 (soft law)	Option 2 (limited)	Option 3 (measured)	Option 4 (far-reaching)	Option 5 (repeal)
Citizens	**0**	≈	✓	✓✓	✓✓✓/×	××
ECS	**0**	≈	≈	✓	✓	✓✓✓
OTTs	**0**	**0**	××	××	×××	**0**
Websites/ OBA	**0**	≈	**0**	✓✓/××	×××	✓✓✓
Browsers/ OS	**0**	**0**	**0**	×××	×××	**0**
Direct marketers	**0**	≈	×	××	×××	✓✓✓
SMEs	**0**	≈	×××	✓✓✓/××	✓✓✓/××	✓✓✓
National authorities	**0**	≈	≈	×	×	**?**
Commission	**0**	×	≈	≈	×	≈

Impact on various categories of stakeholders, ✓✓✓(Strong and positive– ✓✓ (Moderate and positive) – ✓ (Weak and positive) - ×××(Strong and negative) – ××(Moderate and negative) – × (Weak and negative) – ≈ marginal or neutral - ? uncertain; n.a. not applicable. 0 no impact -- ✓/×; ✓✓/××; ✓✓✓/××× (mixed impact: positive + moderate impact at the same time)

ANNEX 14: GLOSSARY

Article 29 Working Party 29

The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

It has advisory status concerning the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures. It acts independently. It is composed of:

- a representative of the supervisory authority (ies) designated by each EU country;
- a representative of the authority (ies) established for the EU institutions and bodies;
- a representative of the European Commission.

The Working Party elects its chairman and vice-chairmen. The chairman's and vice-chairmen's term of office is two years. Their appointment is renewable.

The Working Party's secretariat is provided by the Commission

Communication

Communication means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information[151].

Cookie

A cookie is information saved by the user's web browser, the software program used to visit the web. When visiting a website, the site might store cookies to recognise the user's device in the future when he comes back on the page. By keeping track of a user over time, cookies can be used to customize a user's browsing experience, or to deliver targeted ads. **First-party cookies** are placed by the website visited to make experience on the web more efficient. For example, they help sites remember items in the user shopping cart or his log-in name. **Third-party cookies** are placed by someone other than the site you are on (e.g. an advertising network to deliver ads to the online user) for instance in his browser to monitor his behaviour over time.

Do Not Track standard

The Do Not Track (DNT) policy is an opt-out approach for users to notify web servers about their web tracking preferences. It is opt-out since users have to explicitly state they do not want to be tracked by the website. The DNT policy is implemented technically using an HTTP header field binary option where **1** means the user does not want to be tracked and **0** (default) means the user allows tracking in the website. Web servers can also communicate their tracking status, for example, they only track users with consent, they track users anyway, they disregard the DNT header, etc.

Electronic communications service ("ECS")

[151] Article 2d of the ePD.

Electronic communications service means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks[152].

European Data Protection Board

The General Data Protection Regulation (GDPR) has transformed the Article 29 Working Party into the "European Data Protection Board" ("**EDPB**"). The Members of the Board are those of the Working Party, except the Commission who has the right to participate, and its secretariat is ensured by the European Data Protection Supervisor. The EDPB has been given powers aimed at ensuring consistent approaches by national DPAs, provide advice and guidance.

European Data Protection Supervisor ("EDPS")

The European Data Protection Supervisor is the independent supervisory authority at EU level with responsibility for: (1) monitoring the processing of personal data by the EU institutions and bodies; (2) advising on policies and legislation that affect privacy; (3) cooperating with similar authorities to ensure consistent data protection.

Internet of Things (IoT)

Internet of Things (IoT) represents the next step towards the digitisation of our society and economy, where objects and people are interconnected through communication networks and report about their status and/or the surrounding environment.

Online Behavioural Advertising ("OBA")

Online behavioural advertising involves the tracking of consumers' online activities in order to deliver tailored advertising. The practice, which is typically invisible to consumers, allows businesses to align their ads more closely to the inferred interests of their audience. In many cases, the information collected is not personally identifiable in the traditional sense – that is, the information does not include the consumer's name, physical address, or similar identifier that could be used to identify the consumer in the offline world. Instead, businesses generally use "cookies" to track consumers' activities and associate those activities with a particular computer or device. Many of the companies engaged in behavioural advertising are so-called "network advertisers," companies that select and deliver advertisements across the Internet at websites that participate in their networks.

Over The Top Provider s (OTTs)

An over-the-top (OTT) service provider is essentially an Internet platform that allows communications to be exchanged by the members of the platform, in the form of voice, text or data. These providers do not control the transmission of the messages, but rely on end-users' internet connections for the messages to be relayed.

Location data

Location data means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal

[152] Article 2c of the Framework Directive 2002/21/EC.

equipment of a user of a publicly available electronic communications service.

Personal data breach

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service[153].

Robinson lists (or opt-out lists)

A Robinson list or Mail Preference Service (MPS) list is an opt-out list of people who do not wish to receive marketing transmissions. The marketing can be via e-mail, postal mail, telephone, or fax. In each case, contact details will be placed on a blacklist[154].

Subscriber

Subscriber means any natural person or legal entity who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services[155].

Traffic data

Traffic data means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof[156].

User

User means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service[157].

Value added service

Value added service means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof[158].

[153] Article 2i of the ePD.
[154] Wikipedia.org.
[155] Article 2k of the Framework Directive 2002/21/EC.
[156] Article 2b of the ePD.
[157] Article 2a of the ePD.
[158] Article 2g of the ePD.