# Digitalisation and digital policies in SEE

**SEEDIG 2018 Survey** 

## **About the survey**

#### Why and how?

- The purpose of this survey was to try to capture the perception of the Internet community in South Eastern Europe and the neighbouring area (SEE) on aspects related digitalisation and digital policies across the region.
- It covers topics such as the region's readiness for the digital economy, digital skills, Internet neutrality, cybersecurity, digital rights, and data-driven technologies.
- The survey was conducted online, in April May 2018, by South Eastern European Dialogue on Internet Governance (SEEDIG). The results served as input into the 4<sup>th</sup> SEEDIG annual meeting, held on 23–24 May 2018, in Ljubljana.

#### Key findings (1)

- Countries in SEE are only 'somewhat prepared' to embrace the opportunities of **digitalisation** and digital technologies, according to the majority of survey respondents.
- Among the **top priority areas that countries should focus on to be able to better take advantage of the opportunities of digitalisation**, most respondents indicated digital literacy (70%), addressing the digital divide (68%), and supporting innovation and market growth (62%).
- These areas were also identified as the **most common challenges in SEE**, together with tackling the risks posed by hate speech, extremist content online, and the spread of disinformation (60%), ensuring cybersecurity and combating cybercrime (51%), and protecting human rights online (51%).
- u **Regional cooperation** could significantly help tackle these challenges, according to almost half of the respondents.

#### **Key findings (2)**

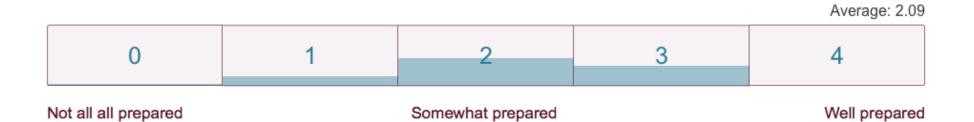
- Specific legislation/regulation is the most effective approach to ensure **network and platform neutrality**, according to 67.9% of the respondents. Market competition (17%) and self-regulation (13.2%) were found to be less effective.
- There is room for improvements when it comes to what stakeholders in SEE are doing to enforce and protect **digital rights**. A majority of respondents indicated that stakeholders' efforts in this area were sufficient 'to some extent' when it comes to protecting freedom of expression and children rights online, but only 'sufficient to a limited extent' in the case of privacy and data protection, gender rights online, and rights of persons with disabilities.
- There is a general feeling of lack of trust in the efficiency of national **cybersecurity** frameworks. Overall, 32% of the respondents indicated they were satisfied with the national frameworks 'to a limited extent', 26% only 'to some extent', and 25% 'not at all'. Data protection, end-users themselves, lack of strategies, and limited awareness and education were indicated as some of the main cybersecurity-related challenges in SEE.

#### Key findings (3)

- Government and individuals themselves share the primary responsibility for advancing digital literacy.
- A proper balance can be achieved, at least to some extent, between protecting users' rights to **privacy and data protection** and the development of the **digital economy**, according to most survey respondents.
- Ethics and human rights considerations were identified as the main challenge associated with advancements in the field of robotics, automation, and artificial intelligence (66%), followed by the impact on the jobs market (60%) and safety and security of automated systems (60%). Privacy and data protection (75%) and cybersecurity (70%) were indicated as the main challenges associated with **Internet of Things** devices.
- All in all, SEE countries can take advantage of the opportunities offered by data-driven technologies if they focus on **education** (77%) and support **innovation and research and development** in these areas (64%).

# 1. Digitalisation: opportunities and challenges

#### 1.1. How prepared would you say your country is to embrace the opportunities of digitalisation and digital technologies?



### 1.2. What priority areas should your country focus on to be able to better take advantage of the opportunities of digitalisation?

1	Promoting digital literacy	70%
2	Addressing the digital divide, in its various forms (infrastructure availability, affordability of access, etc.)	68%
3	Supporting innovation and market growth	62%
4	Tackling the risks posed by hate speech, extremist content online, and the spread of disinformation	49%
5	Protecting human rights online	43%
6	Ensuring cybersecurity and combating cybercrime	42%
7	Countering hybrid threats	11%
8	Other	2%

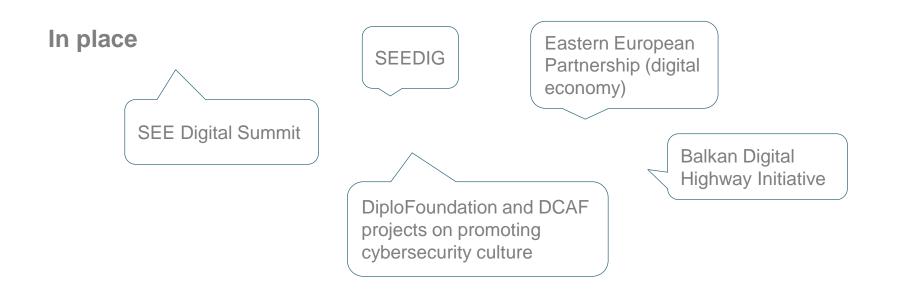
## 1.3. What common challenges do the countries in SEE face in the process of digitalisation?

1	Addressing the digital divide, in its various forms (infrastructure availability, affordability of access, etc.)	70%
2	Promoting digital literacy	66%
3	Supporting innovation and market growth	62%
4	Tackling the risks posed by hate speech, extremist content online, and the spread of disinformation	60%
5	Ensuring cybersecurity and combating cybercrime	51%
6	Protecting human rights online	51%
7	Countering hybrid threats	32%
8	Other	2%

1.4. Could regional cooperation (among countries and among different stakeholders) help tackle the challenges identified above in a more effective and efficient manner?



#### 1.5. Examples of successful regional cooperation in addressing challenges related to digitalisation



#### Suggested

Working groups to collaborate on addressing legal and practical issues

Sharing of experiences

Regional e-services platforms

## 2. Digital skills

## 2.1. How important is digital literacy today compared to conventional literacy and numeracy?

1	Equally important	70%
2	Significantly more important	30%
3	Less important	0%
4	Not at all	0%

#### 2.2. What competencies are covered by the term 'digital literacy'?

1	Effective use of online services and applications	4 89%
2	Effective use of devices	72%
3	Online communication and collaboration	72%
4	Safe Internet use	72%
5	Digital identity management	66%
6	Information search and sharing	66%
7	Online learning and self-development	60%
8	Creative use of technology	30%
9	Other	2%

#### 2.3. How would you assess your digital literacy and readiness?

1	Advanced	57%
2	Medium	30%
3	I don't know how to measure	13%
4	Low	0%

#### 2.4. Who bears the highest responsibility for advancing individual digital literacy?

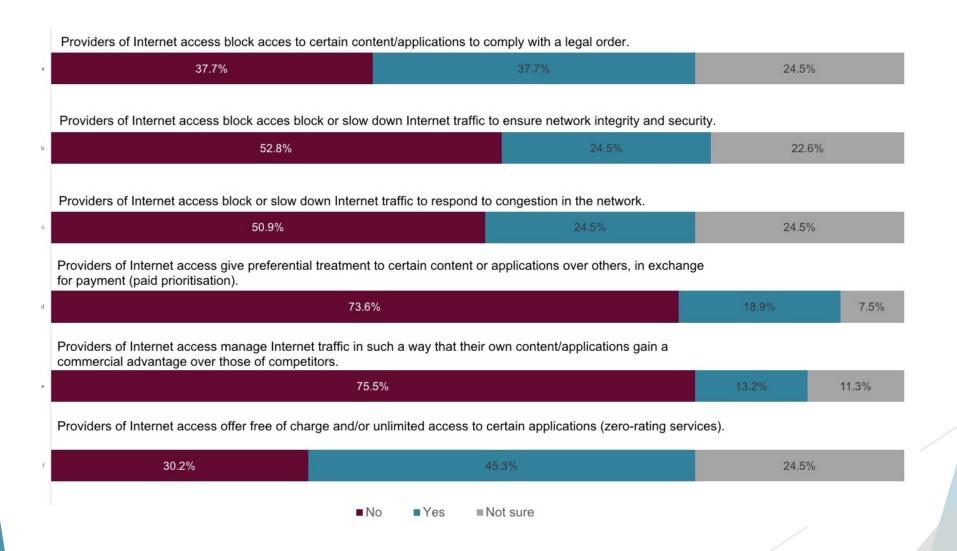
1	Governments	75%
2	Individual users themselves	74%
3	Academia	55%
4	Civil society	49%
5	Technology companies	32%

# 3. From network to platform neutrality

#### 3.1. If network neutrality is protected by law/regulation in your country, how effective is the enforcement of these rules?

1	To some extent	36%
2	There is no law/regulation	30%
3	Significantly	13%
4	To a limited extent	11%
5	Not at all	9%

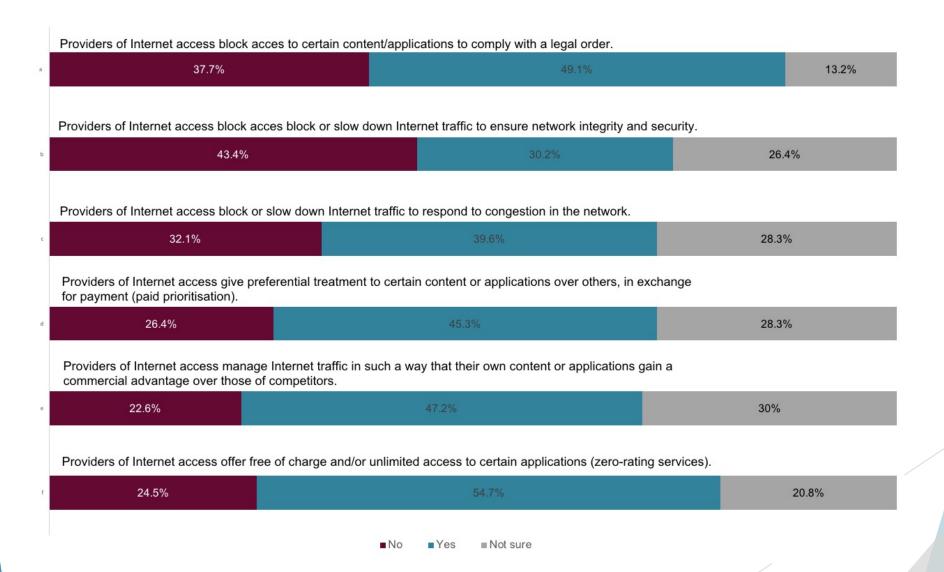
#### 3.2. As a user of digital technologies, do you consider the practices below to be acceptable?



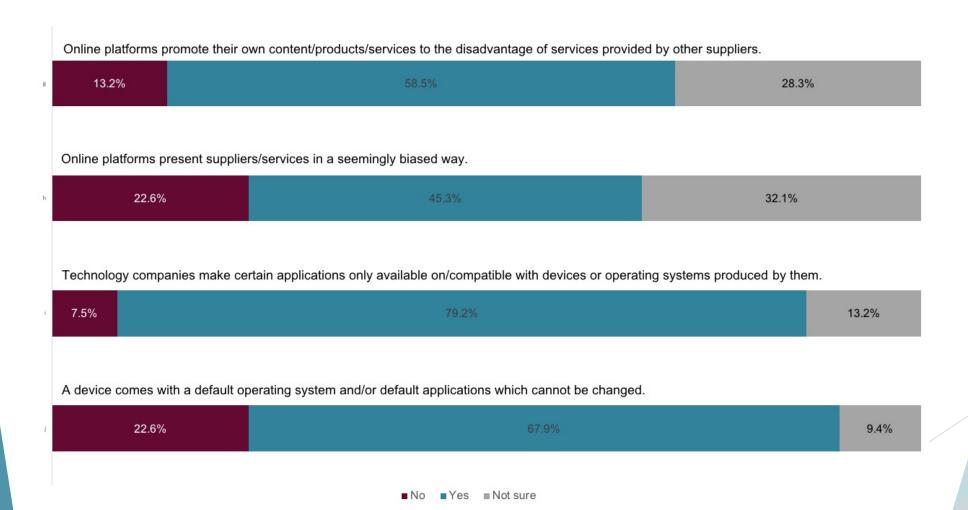
#### 3.2. As a user of digital technologies, do you consider the practices below to be acceptable? (cont.)

Online platforms promote their own content/products/services to the disadvantage of services provided by other suppliers. 49.1% 26.4% Online platforms promote certain content/products/services in exchange for payment (paid prominence or sponsored ranking). 30.2% 18.9% Technology companies make certain applications only available on/compatible with devices or operating systems produced by them. 17% 56.6% Device manufacturers do not allow users to change default operating systems or install applications from other suppliers. 20.8% 64.2% ■ Not sure

#### 3.3. As a user of digital technologies, have you experienced any of the following practices?



#### 3.3. As a user of digital technologies, have you experienced any of the following practices? (cont.)

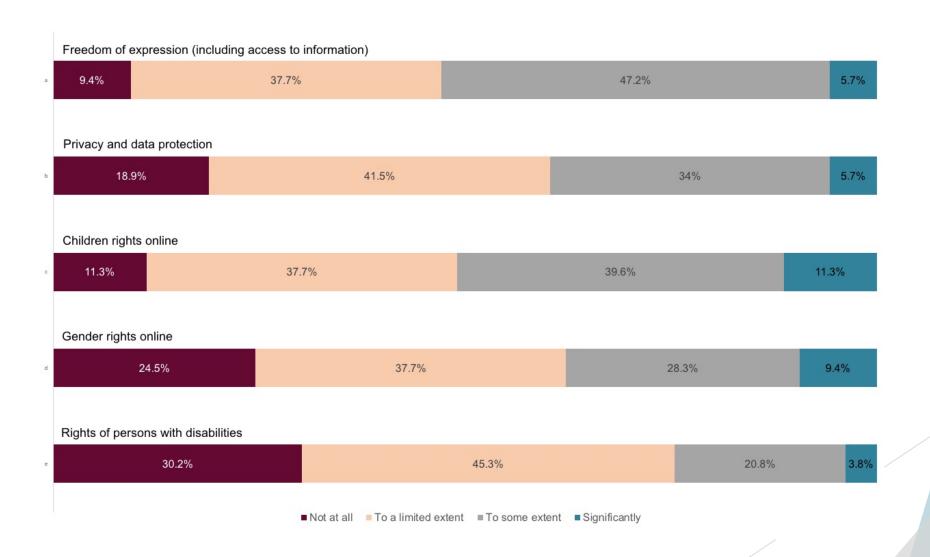


## 3.4. What would be the most effective approach to ensure network and platform neutrality?

1	Specific legislation/regulation	68%
2	Market competit <mark>ion</mark>	17%
3	Self-regulati <mark>on</mark>	13%
4	Other	2%

## 4. Digital rights: awareness and enforcement

#### 4.1. Do you consider that stakeholders in SEE are doing enough to enforce and protect the following digital rights?



### 4.2. What are the main challenges to ensuring a better protection of digital rights in your country and in SEE?

C	Limited trust in the government and the private sector to prioritise the protection of digital rights	66%
	digital rights	
1	Not enough responsibility on the part of the private sector	45%
F	Finding a balance between potentially conflicting state interests (e.g. the need to protect freedom of expression and the need to combat hate speech)	42%
0	Other	2%

### 4.3. In your view, in which circumstances can freedom of expression (including access to information) be limited online?

1	Dealing with hate speech and extremist content	77%
2	Combating disinformation	60%
3	Protecting intellectual property rights	57%
4	Ensuring morality and public order	28%
5	Other	6%

Criminal content

### 4.4. How can we best deal with the challenges and risks associated with the use of digital technologies by children?

1	Education and awareness on child safety online in schools	94%
2	Parental awareness and capacity building	94%
3	Parental control of children's Internet access	53%
4	Awareness campaign by Internet companies	49%
5	Restricting children's access to the Internet	23%
6	Other	4%

4.5. Would you say that your government has taken steps to implement gender-responsive ICT policies (e.g. policies which include targets or plans to improve women's access and digital skills)?



#### **Examples of gender-responsive ICT policies**

Oirls in IT Day

New legislation on digital rights, including gender rights

Participation in Global Network of Women in ICT, support to women's business in ICT through programmes of start-up and innovative loans, a special programme for training and re-training women into the ICT sector.

## 5. Cybersecurity

5.1. Whose primary fault is it for the occurrence of cybersecurity incidents and cybercrime acts such as data breaches, hacking, and ransomware?



#### 5.1. Whose primary fault is it for the occurrence of cybersecurity incidents and cybercrime acts such as data breaches, hacking, and ransomware? (cont.)

#### Others responsible

Multiple stakeholders.
Cybersecurity is
everyone's
responsibility.

Criminals Hackers

Crime will always exist, it has just expanded to digital space.

Neglecting the importance of updating the systems being used by everyone mentioned. Vendors also have their responsibility in placing in the market products that lack security mechanisms.

We can not talk about a specific fault. The Internet was established as an open technology platform. On the one hand, this represents an exceptional opportunity for innovation and development; on the other hand, it brings a number of security risks.

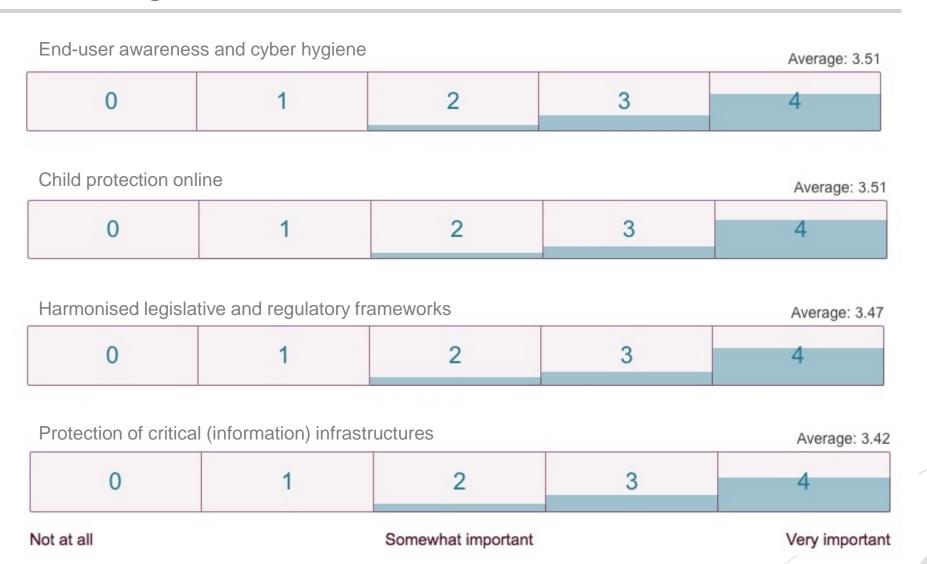
Human behavior on all sides, when the Internet becomes mass media.

### 5.2. How satisfied are you with your country's cybersecurity framework (strategies, legislation, dedicated institutions, etc.)?

1	To a limited extent	32%
2	To some extent	26%
3	Not at all	25%
4	Not sure what my country's cybersecurity fr	ramework is or whether there is one at all 13%
5	Significantly	4%



#### 5.4. How important are the following issues when it comes to cybersecurity priorities in the SEE regional context?



## 5.4. How important are the following issues when it comes to cybersecurity priorities in the SEE regional context? (cont)

Cyber-defence				Average: 3.32
0	1	2	3	4
Broader regional co	operation			Average: 3.32
0	1	2	3	4
Combating cybercri	me			Average: 3.26
0	1	2	3	4
Performant Comput	er Emergency Resp	onse Teams (CERTs)		Average: 3.26
0	1	2	3	4
Public-private partn	erships			Average: 3.06
0	1	2	3	4
Not at all	1	Somewhat important		Very important

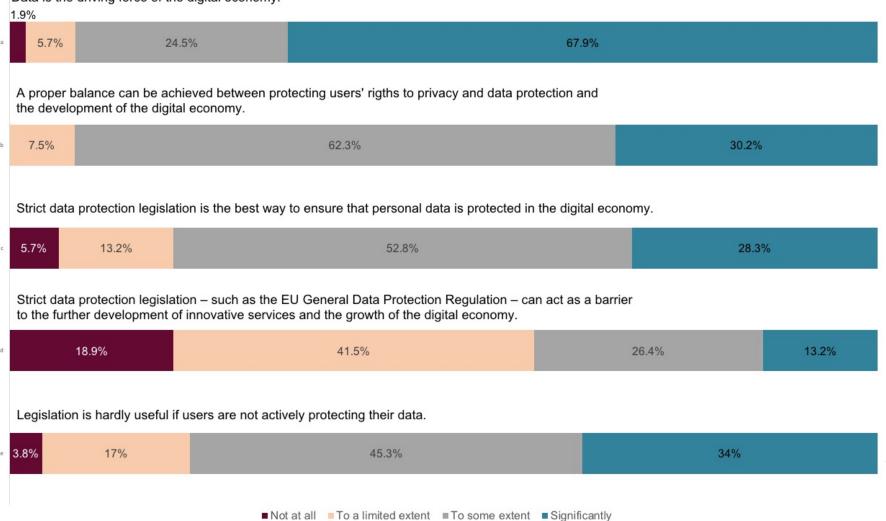
## 6. Data economy

#### 6.1. Privacy and data protection in the digital space is the main responsibility of:

1	Internet companies that collect and process data	79%
2	Governments and law enforcement agencies	75%
3	End-users	49%
4	Providers of Internet access	42%
5	Other	2%

#### 6.2. Data protection in the digital economy: To what extent do you agree with...?

Data is the driving force of the digital economy.



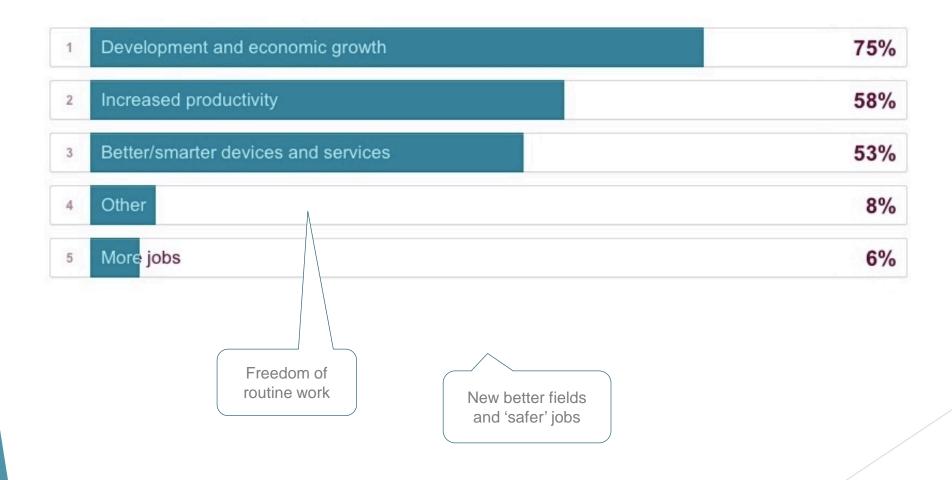
## 6.3. When it comes to guaranteeing users' right to privacy and data protection, the main responsibility of Internet companies lies in:

1	Informing users when their data have been compromised	79%
2	Being completely transparent about how personal data is used	75%
3	Making terms of services easy to read and understand	66%
4	Being ethically responsible towards their users, even if that means taking measures not required by legislation	64%
5	Respecting the law, nothing more or less	28%
6	Other	2%

There are no guaranties for privacy from Internet companies. It's not on them only, but on all involved.

# 7. Data-driven technologies

#### 7.1. What are the main benefits that come with advancements in the field of robotics, automation, and AI?



## 7.2. What are the main challenges that come with advancements in the field of robotics, automation, and artificial intelligence (AI)?

1	Ethics and human rights considerations in the design of AI systems	66%
2	Jobs lost and the workforce not being prepared for the new labour market demands	60%
3	Safety and security in the framework of automated systems such as self-driving cars	60%
4	Liability and responsibility when it comes to decisions made by AI systems	58%
5	Increasing social inequalities, as some take advantage of the new technologies, while others are left behind	53%
6	Other	4%

These 'robots' some day maybe will be out of control.

#### 7.3. What are the main challenges associated with Internet of Things (IoT) devices?

1	Privacy and data protection	75%
2	Cybersecurity	70%
3	Connectivity issues (insufficient/inadequate infrastructures to support IoT devices)	45%
4	Lack of/limited interoperability between devices from different vendors	36%
5	Environmental concerns (energy usage)	26%
6	Other	2%

## 7.4. Can countries in SEE take advantage of the opportunities offered by data-driven technologies (Al, IoT, blockchain, etc.)?

1	Yes, if they focus on education and formation to ensure that today's and tomorrow's workforce is prepared for the new and emerging world of work.	77%
2	Yes, if they support innovation, research, and development in these technologies.	64%
3	Probably not, and we will face new forms of digital divides within the region, and in comparison with other regions.	17%

# 8. Technical issues: IDNs and IPV6

## 8.1. Should the Internationalised Domain Names (IDNs) be better promoted in the SEE region?

1	Yes, because they promote multilingualism and cultural diversity.	57%
2	Yes, because they can help bring more people online.	45%
3	No, because there are still unresolved technical issues.	25%
4	No, because they can lead to fragmentation of the Internet.	8%
5	No, because they create confusion.	8%

## 8.2. Who bares the main responsibility for improving Internet Protocol version 6 (IPv6) adoption in SEE?





Education.
Players in SEE
are not aware of
IPv6.

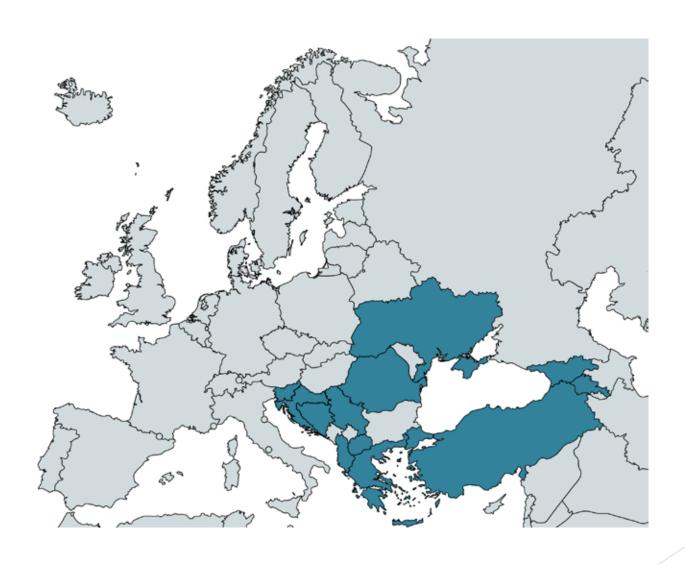
Users

Non-governmental technical associations.

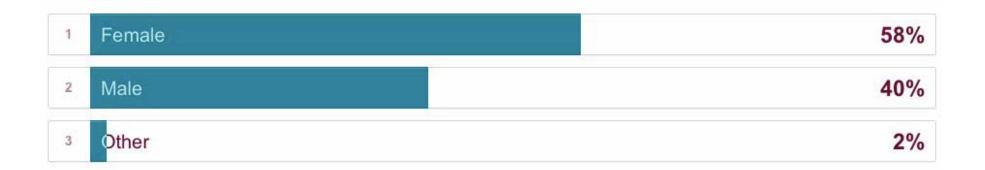
# 9. Demographics

#### 9.1. Stakeholder group of respondents

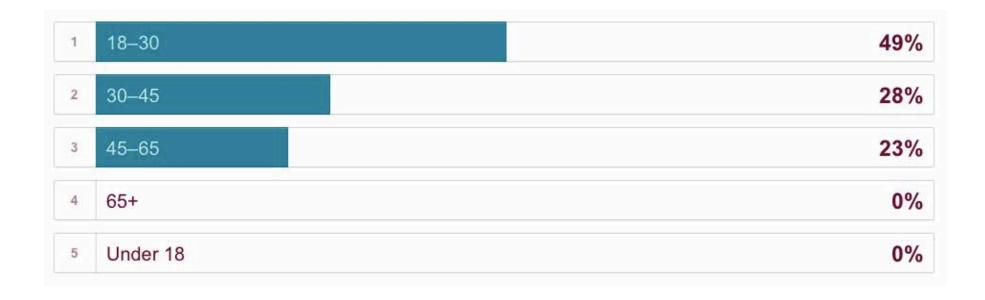
1	Civil society	38%
2	Academia	17%
3	Technical community	15%
4	Government	11%
5	Private sector	11%
6	Media	6%
7	Intergovernmental organisation	2%



#### 9.3. Gender of respondents



#### 9.4. Age of respondents



## **Final notes**

More details about the survey are available at http://seedig.net/survey-2018-digitalisation/.

For any queries, please contact us at execom@seedig.net.



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License https://creativecommons.org/licenses/by-sa/4.0/