

DATA PRIVACY TRENDS IN EU: AN OVERVIEW OF RECENT DEVELOPMENTS

Cristina ANTONOAIIE*, Mihai ALEXANDRESCU**

* Regional Department of Defense Resources Management Studies,
Brasov, Romania

** Spiru Haret University Bucharest, Faculty of Economic Sciences and
Juridic Sciences Brasov, Romania

The article highlights growing trends in data privacy behaviors among internet users, in the EU. People are increasingly limiting cookies and tracking, using privacy protection software, and reading privacy policies before sharing personal data. Many are also restricting geolocation access, limiting social media profile visibility, and refusing to allow their data to be used for advertising. Additionally, users are more cautious about website security, checking for HTTPS before entering sensitive information. These behaviors reflect heightened awareness of data protection and a desire to safeguard personal information in response to concerns about privacy, surveillance, and online tracking. This shift is influenced by regulations like GDPR and the growing mistrust of data exploitation practices.

Key words: *privacy, behavior, challenges, regulation, solutions*

INTRODUCTION

The EUROSTAT database, within the item Digital Economy and Society, has provided us with some information about individuals' behavior regarding trust, security, and privacy when navigating the internet. We analyzed this behavior in 8 different situations using the most recent data available, that of 2023.

Firstly, individuals have changed the settings in their internet browser to prevent or limit cookies on any

of their devices. This reflects an increasing trend of individuals taking control of their privacy. With growing concerns over tracking and data harvesting by advertisers and websites, this indicates a shift towards greater online privacy awareness and proactive data protection.

Secondly, individuals use software that limits the ability to track their activities on the internet. The use of privacy-enhancing software is becoming more widespread as people seek to minimize their digital footprint. Tools like VPNs, ad-

blockers, and browser extensions help users reduce online tracking, which aligns with increasing public awareness about the need for anonymity and security while browsing.

Thirdly, individuals manage access to personal data on the internet (3 months): read privacy policy statements before providing personal data. More users are now scrutinizing privacy policies before sharing personal information, which indicates a growing understanding of the risks associated with sharing personal data. However, the challenge remains that many privacy policies are complex and difficult to interpret, suggesting room for improvement in terms of clarity and transparency.

Fourthly, individuals manage access to personal data on the internet (3 months): restricted or refused access to the geographical location. The refusal to share geolocation data is a strong sign of privacy-conscious behavior. Many users are becoming aware of the risks involved with location tracking, which can be used for intrusive advertising and surveillance. This trend reflects a desire for greater control over personal information and where it's shared.

Fifthly, individuals manage access to personal data on the internet (3 months): limited access to profile or content on social networking sites or shared online storage. Users

are increasingly cautious about the privacy of their social media profiles and content. By limiting access to personal information, they are taking steps to protect themselves from data breaches, misuse, and the commercialization of their personal data. This trend highlights the growing demand for more privacy on social media platforms.

Sixthly, individuals manage access to personal data on the internet (3 months): refused allowing the use of personal data for advertising purposes. Many individuals are opting out of having their data used for personalized advertising. This is a response to concerns over the commercialization of personal data and a growing mistrust of targeted advertising techniques. It underscores the desire for more autonomy over personal information and how it's utilized.

Seventhly, individuals manage access to personal data on the internet (3 months): checked that the website where personal data provided was secure. The practice of checking website security (e.g., looking for HTTPS) before submitting sensitive data is a crucial step in protecting personal information. This trend reflects an increasing awareness of cybersecurity threats, as users are more cautious about where and how they provide their personal information.

Eighthly, Individuals manage access to personal data on the internet

(3 months): at least one of I_MAPS_RPS [1], I_MAPS_RRGL [2], I_MAPS_LAP [3], I_MAPS_RAAD [4], I_MAPS_CWSC [5]. This indicates that individuals are actively engaging with various privacy and security measures, such as using privacy-enhancing tools, adjusting settings, or refusing certain data uses. This overall behavior shows that privacy has become a priority for many users, with a shift toward more informed and deliberate online actions to safeguard their personal data.

2. DATA ANALYSIS

2.1. Percentage of individuals that have changed the settings in their internet browser to prevent or limit cookies on any of their devices in 2023

Bulgaria is the only country in the category (less than 10%), indicating a low level of awareness or interest in online data protection among users in this country. Possible factors include a lack of digital education, less concern about privacy, or lower access to information about privacy options.

Cyprus and Romania (10.31%) fall into the category 10 – 20%, suggesting a moderate level of interest in online data protection, but not to the extent of other European countries. There could be factors such as partial digital education, lower awareness of the risks associated with cookies, or regulatory differences that influence this behavior.

This category (20 – 30%) includes a wide range of countries, such as France, Italy, and Poland.

Table 1 Percentage of individuals that have changed the settings in their internet browser to prevent or limit cookies on any of their devices in 2023

% of individuals 2.1.	Countries	No of countries
less than 10	BG	1
10-20	CY, RO	2
20-30	EL, FR, HR, IT, LT, LV, PL, SI, SK	9
30-40	AT, BE, CZ, EE, ES, HU, MT, PT, SE	9
40-50	DE, DK, IE, LU	4
more than 50	FI, NL	2
Total		27

It's evident that in these countries there is a greater concern for online privacy, and more users are choosing to control or limit cookies. These countries may have stronger educational initiatives or stricter data protection regulations, such as GDPR.

In this category (30 – 40%), countries such as Sweden, Spain, and Belgium have a significantly higher percentage of users modifying their browser settings for data protection. These countries typically have strong data protection infrastructures and a more educated population regarding their online privacy rights. These percentages suggest proactive user behavior in protecting their personal data.

Germany, Denmark, Ireland, and Luxembourg are countries with a high level (40 – 50%) of awareness of data protection and strict privacy policies. These countries likely benefit from strong educational campaigns and stringent privacy regulations,

leading a significant number of users to adjust their browser settings to control cookies.

Finland and the Netherlands top this list, with more than half of users choosing to modify their settings for online data protection. These countries have a high level of digital education and awareness of privacy rights. They also have a strong culture of privacy and data protection compliance. On the whole, most European countries are in the mid-range for online privacy interest, but there are clear examples of countries with high interest, such as Finland and the Netherlands. Data protection policies, national regulations, and digital education significantly influence user behavior in this regard.

2.2. Percentage of individuals that use software that limits the ability to track their activities on the internet in 2023

Table 2 Percentage of individuals that use software that limits the ability to track their activities on the internet in 2023

% of individuals 2.2.	Countries	No of countries
less than 8	BG, CY	2
8-16	CZ, EL, IT, LV, RO, SI	6
16-24	AT, DE, ES, FR, HU, LT, PL, PT, SK	9
24-32	DK, EE, FI, HR, IE, LU, SE	7
32-40	MT, NL	2
more than 40	BE	1
Total		27

Bulgaria and Cyprus are the two countries in the category (less than 8%), showing a very low adoption of privacy software. This suggests that in these countries, online privacy concerns may not be as prominent among users. Possible factors for this low percentage could include less awareness of online privacy issues, limited access to privacy tools, or a lower level of digital literacy regarding how tracking works and how to avoid it.

Czech Republic, Greece, Italy, Latvia, Romania (10.42%), and Slovenia are in this range (8 – 16%), indicating a moderate but still relatively low usage of privacy-protecting software. The fact that these countries are adopting such tools at a higher rate compared to the previous group shows growing awareness of the importance of online privacy. However, the adoption rate suggests that while there is some interest in online privacy protection, it may still be overshadowed by other concerns like general internet usage habits or the lack of easily accessible, user-friendly tools.

Countries like Austria, Germany, Spain, France, Hungary, Lithuania, Poland, Portugal, and Slovakia fall into the category (16 – 24%). This indicates a stronger uptake of privacy software. The relatively higher usage in these countries could be attributed to increased awareness of data protection issues,

including privacy scandals, such as the Cambridge Analytica incident or the implementation of the GDPR (General Data Protection Regulation) in the EU, which has raised awareness around user rights and privacy online. In these countries, users are likely to be more informed about the risks associated with online tracking and may have more access to tools that can help them safeguard their privacy, especially with ongoing digital education initiatives and stronger regulatory frameworks.

The countries in this category – Denmark, Estonia, Finland, Croatia, Ireland, Luxembourg, and Sweden – have a significant proportion of individuals (24 – 32%) using privacy-protecting software, indicating a more robust commitment to online privacy. These countries have generally high levels of digital literacy, education on online privacy, and strong privacy regulations in place. For example, Estonia and Finland are known for their advanced digital infrastructures, while Sweden and Denmark have a long-standing tradition of valuing data protection and privacy. The adoption rate suggests that these countries are likely leading the way in terms of educating users about the importance of privacy tools and providing them with accessible means to protect themselves.

Malta and the Netherlands are the only countries in this category (32 – 40%). This relatively high

percentage of users adopting privacy software reflects a strong digital culture focused on personal data protection. The Netherlands, in particular, is known for its high level of privacy awareness and is home to some of the strictest privacy laws in Europe. Malta, though smaller, may also have strong privacy laws and a tech-savvy population. This high percentage may also be due to proactive government policies, privacy advocacy groups, and a digital population that values their privacy rights. These countries likely have high levels of trust in their privacy tools and an informed user base that actively seeks to protect their data.

Belgium stands alone in this category, with over 40% of individuals using software to limit

tracking. This is a notable figure, showing that privacy awareness and action are highly prioritized in Belgium. Belgium benefits from a combination of high digital literacy, active privacy advocacy, and strong regulatory frameworks, particularly as part of the European Union's GDPR-compliant policies. The high usage of privacy tools here suggests that users are very proactive about their online security and privacy, possibly due to a deep cultural and governmental focus on data protection and rights.

2.3. Percentage of individuals that manage access to personal data on the internet (3 months): read privacy policy statements before providing personal data in 2023

Table 3 Percentage of individuals that manage access to personal data on the internet (3 months): read privacy policy statements before providing personal data in 2023

% of individuals 2.3.	Countries	No of countries
less than 21	BE, CY, FR, LU	4
21-26	SI	1
26-31	EL, PL, RO, SE	4
31-36	BG, CZ, DE, DK, IT, LV	6
36-41	EE, ES, HR, IE, LT, MT, PT, SK	8
more than 41	AT, FI, HU, NL	4
Total		27

Belgium, Cyprus, France, and Luxembourg fall into this category, with fewer than 21% of individuals reading privacy policy statements before sharing personal data. This indicates a relatively low level of privacy awareness in these countries. While these countries have access to privacy policies and data protection regulations, it appears that many individuals are not fully engaging with them. Possible reasons could include a lack of understanding of the importance of privacy policies, low awareness of the risks associated with sharing personal data, or a general trust in the services they use. Despite the existence of strong regulations like GDPR in the European Union, it seems that not all individuals prioritize reading the terms before providing their personal information.

Slovenia is the only country in this range, with 21-26% of individuals checking privacy policies before providing personal data. This reflects a somewhat moderate level of privacy-conscious behavior, although still on the lower end. It suggests that while there is some awareness, privacy concerns are not yet a widespread practice for most Slovenian internet users. Slovenia may have a growing awareness of privacy and data protection, but like many other countries, there may be competing factors such as convenience and trust in online platforms, leading users to overlook reading privacy policies.

Greece, Poland, Romania (30.73%), and Sweden are in this category, with 26-31% of individuals reading privacy policies before sharing personal data. This shows a moderate level of privacy awareness. The higher percentage in Sweden could be attributed to its strong culture of digital rights and a population more aware of privacy issues due to a high level of digital education and government focus on data protection. In contrast, countries like Greece, Poland, and Romania may still be developing stronger privacy practices, with users showing some concern but not yet engaging with privacy policies on a regular basis.

Bulgaria, Czech Republic, Germany, Denmark, Italy, and Latvia are in this range, where 31-36% of individuals are reading privacy policy statements before providing personal data. This percentage indicates a moderate-to-high level of privacy engagement, suggesting that people in these countries are more aware of the importance of protecting their personal information online. Germany and Denmark are notable for their strong privacy regulations (such as GDPR) and culture, which likely contributes to the higher percentage in these countries. However, there is still room for improvement in other countries in this range, like Bulgaria and Czech Republic, where data privacy concerns may not be as widespread or deeply ingrained.

Countries like Estonia, Spain, Croatia, Ireland, Lithuania, Malta, Portugal, and Slovakia show a higher level of engagement with privacy policies, with 36-41% of individuals reading them before sharing their personal data. This reflects a growing trend toward online privacy awareness and self-protection. Estonia, known for its advanced digital infrastructure, leads the way in digital literacy and data protection. Spain and Ireland also benefit from strong awareness and regulatory frameworks. This indicates that individuals in these countries are becoming more proactive in managing their personal data, perhaps as a result of digital literacy campaigns, data protection laws, and public concern about privacy risks.

Austria, Finland, Hungary, and the Netherlands are the countries in this category, with over 41% of individuals reading privacy policies

before providing their personal data. This is the highest level of engagement, showing that these countries have a particularly high awareness of privacy issues. Finland and the Netherlands are known for their strong data protection laws and high levels of digital literacy, leading to a population that is well-versed in privacy rights and protections. In these countries, individuals seem to be actively seeking to manage their personal data and make informed decisions about their privacy online. The high percentage also suggests that privacy is a key concern for these users, and they may take extra steps to ensure they are informed about how their data will be used.

2.4. Percentage of individuals that manage access to personal data on the internet (3 months): restricted or refused access to the geographical location in 2023

Table 4 Percentage of individuals that manage access to personal data on the internet (3 months): restricted or refused access to the geographical location in 2023

% of individuals 2.4.	Countries	No of countries
less than 22	BG	1
22-33	LV, RO, SI	3
33-44	CY, DE, EL, HR, IT, LT, PL, SK	8
44-55	AT, BE, CZ, EE, HU, LU, MT, PT	8
55-66	DK, ES, FR, IE, SE	5
more than 66	FI, NL	2
Total		27

Bulgaria has the lowest percentage in this category, with fewer than 22% of individuals restricting or refusing access to their geographical location. This suggests that privacy concerns related to location tracking are relatively low in Bulgaria, and many users might not be aware of or concerned about the risks of sharing their geographical data. Possible reasons for this could include a lack of privacy education, less emphasis on location-based data privacy, or a general trust in digital platforms. Users in Bulgaria might have less awareness of the risks related to location data. There may be fewer readily accessible tools or resources that allow Bulgarians to manage or limit location access and they may be more focused on other internet usage concerns, such as access to services or convenience, rather than restricting location sharing.

Latvia, Romania (26.60%), and Slovenia fall into this range, with 22-33% of individuals restricting or refusing access to their geographical location. This range suggests a moderate level of privacy concern regarding location tracking in these countries. Latvia and Romania might have lower levels of privacy awareness than other EU countries, which could explain the moderate engagement with location restrictions. Slovenia may be slightly more advanced in privacy awareness but still shows room for

improvement. In these countries there is likely a rising awareness of the risks of sharing location data, especially with the growth of location-based services. GDPR has likely raised awareness, but these countries might still be developing stronger digital literacy and tools for location data management.

Cyprus, Germany, Greece, Croatia, Italy, Lithuania, Poland, and Slovakia fall into the 33-44% range. This indicates a stronger, though still moderate, level of concern about location privacy. These countries exhibit a more noticeable engagement with privacy tools to restrict geographical location access, especially in comparison to the first two categories. Germany is likely a standout here, with a long tradition of data protection laws, including GDPR, which has fostered awareness about the risks of location tracking. Cyprus and Greece, while improving, still show moderate privacy practices, which could be related to a combination of trust in local services and a lack of active privacy education.

Countries like Austria, Belgium, Czech Republic, Estonia, Hungary, Luxembourg, Malta, and Portugal fall within this range (44 – 55%). This suggests that in these countries, around half of the population is actively managing their geographical data privacy by restricting or refusing access to location data. Estonia

is a clear leader in digital privacy practices, known for its advanced digital services and a culture of privacy protection. Other countries like Austria and Luxembourg are likely to have higher digital literacy and privacy-conscious populations due to strong legal frameworks such as GDPR. Citizens in these countries are likely more aware of the risks associated with location data sharing and are more proactive in managing access to their geographical location. These countries often have high levels of digital literacy, as well as tools that make it easier for users to manage privacy settings. The presence of comprehensive data protection laws like GDPR in many of these countries contributes to higher engagement with privacy tools.

Countries such as Denmark, Spain, France, Ireland, and Sweden fall into the 55-66% range, where more than half of the population restricts or refuses access to their geographical location. These countries show a high level of concern for privacy and indicate that managing location data is an important issue for many users. Denmark and Sweden are particularly well-known for their strong privacy laws and digital literacy. France and Spain have seen increasing privacy awareness, particularly in light of various high-profile data breaches and scandals, motivating users to be more protective of their location data. Scandinavian countries like Denmark and Sweden are generally

at the forefront of privacy rights, with a strong focus on user control over personal data. These countries have strong privacy laws, which are enforced, and digital literacy campaigns that help users understand the risks associated with sharing location data. Given the number of high-profile privacy incidents across Europe, users in these countries are increasingly cautious about sharing personal data.

Finland and the Netherlands are the leading countries in this category, with over 66% of individuals restricting or refusing access to their geographical location. These countries demonstrate the highest level of awareness and action regarding location privacy. Finland is particularly notable for its advanced digital infrastructure and strong privacy protections. The Dutch population is known for being highly informed about their digital rights and has a long history of advocating for privacy and data protection. Both Finland and the Netherlands have a culture that strongly emphasizes personal privacy, digital rights, and data protection. These nations often lead the way in adopting digital privacy tools and creating a privacy-conscious population. Citizens in these countries are highly informed about privacy and understand the potential risks of sharing location data, leading them to be more proactive in managing their privacy settings.

2.5. Percentage of individuals that manage access to personal data on the internet (3 months): limited access to profile or content on social networking sites or shared online storage in 2023

knowledge or skills to manage their privacy settings effectively.

Countries like Bulgaria, Germany, Greece, Italy, Latvia, Poland, Slovenia, and Slovakia fall into the 20-31% range, indicating a

Table 5 Percentage of individuals that manage access to personal data on the internet (3 months): limited access to profile or content on social networking sites or shared online storage in 2023

% of individuals 2.5.	Countries	No of countries
less than 20	RO	1
20-31	BG, DE, EL, IT, LV, PL, SI, SK	8
31-42	AT, BE, CY, EE, FR, HR, HU, LT, LU,	9
42-53	DK, IE, MT, SE	4
53-64	CZ, ES, FI, PT	4
more than 64	NL	1
Total		27

Romania (19.65%) has the lowest percentage, with fewer than 20% of individuals limiting access to their profile or content on social networking sites or shared online storage. This suggests that in Romania, many users are either unaware of the privacy risks associated with social networks or may not feel the need to control the access to their personal data online. There may be a cultural tendency to share more openly or a lack of emphasis on digital privacy education. Digital privacy tools and settings on social platforms can be complicated to navigate. Users may not be equipped with the necessary

moderate level of concern for privacy on social networking sites and shared online storage. Around one-quarter to one-third of individuals in these countries are actively managing their personal data by limiting access to their profiles or content.

Germany, being a leader in privacy law with GDPR, likely stands out in this group, with higher awareness about data protection and personal privacy. However, countries like Bulgaria, Greece, and Slovakia might be at earlier stages in adopting robust privacy practices, with a lower percentage of individuals actively managing access. These countries

have varying levels of digital literacy. Some may have strong privacy education programs, while others might not. People in these countries might trust social media platforms and may not see the need to limit access unless prompted by negative experiences or data breaches.

Austria, Belgium, Cyprus, Estonia, France, Croatia, Hungary, Lithuania, and Luxembourg fall within this range (31 – 42%). These countries have a higher percentage of individuals who actively manage their privacy settings by restricting access to personal data on social networks and online storage. France and Estonia are likely to have higher levels of digital literacy and a stronger focus on privacy, especially given the prominence of GDPR. Luxembourg and Austria also have strong privacy laws in place, encouraging individuals to be more proactive about managing their personal data. The influence of GDPR plays a significant role in shaping privacy behavior in these countries. Citizens in these countries might feel that the tools and settings available to them on social platforms are reliable and can help them manage their privacy effectively.

Denmark, Ireland, Malta, and Sweden have a more pronounced percentage (42-53%) of individuals managing their privacy settings on social media and online storage platforms. This range reflects a high level of concern for data

protection and a strong trend toward taking proactive steps in managing online privacy. Sweden and Denmark are known for their robust privacy laws and high digital literacy. These countries often lead in global rankings for privacy and data protection, and the population is well-informed about the risks of oversharing online. The presence of user-friendly privacy tools and resources encourages individuals to limit access to their personal data. These countries often have higher levels of digital literacy, making it easier for citizens to understand and implement privacy measures.

Czech Republic, Spain, Finland, and Portugal show a strong commitment to managing access to personal data on social networks and online storage, with 53-64% of individuals limiting access. These countries are likely to have a higher level of concern about online privacy and the risks associated with personal data exposure. Finland and Spain stand out in this group, with Finland having a high level of digital literacy and strong privacy practices. Spain has also seen an increase in privacy awareness due to recent scandals and increased regulation. The influence of GDPR and national privacy laws is likely significant in these countries. Increased awareness around online privacy risks, including potential data breaches and misuse, has led to more individuals taking action to protect their data.

The Netherlands is the only country in this category, with more than 64% of individuals actively limiting access to their profile or content on social networking sites or online storage platforms. This high percentage reflects a high level of privacy awareness and a strong culture of data protection. The Netherlands is known for its strong privacy laws, including GDPR implementation, and a population that is highly aware of digital rights and privacy risks. The Netherlands has a well-established infrastructure for data protection, and individuals are confident in using privacy settings to manage their online data.

2.6. Percentage of individuals that manage access to personal data on the internet (3 months): refused allowing the use of personal data for advertising purposes in 2023

Bulgaria is the only country with fewer than 20% of individuals refusing to allow the use of their personal data for advertising purposes. This indicates that a large majority of people in Bulgaria may either be unaware of the risks associated with data sharing for advertising or may not actively take steps to refuse this practice. Digital privacy issues might not be as pressing or well understood by the population in Bulgaria, especially regarding targeted advertising. Bulgarians may not be aware of available settings or options to limit advertising tracking, or they may trust advertisers more than individuals in countries with higher percentages of refusal.

Latvia and Romania (28.39%) fall within this range, where around 20-30% of individuals refuse the use of their personal data for advertising

Table 6 Percentage of individuals that manage access to personal data on the internet (3 months): refused allowing the use of personal data for advertising purposes in 2023

% of individuals 2.6.	Countries	No of countries
less than 20	BG	1
20-30	LV, RO	2
30-40	PL, SI, SK	3
40-50	BE, DE, EE, EL, HR, HU, IT, LT, LU, MT	10
50-60	AT, CY, CZ, FR, PT, SE	6
more than 60	DK, ES, FI, IE, NL	5
Total		27

purposes. This shows that while some awareness of privacy issues exists, a significant portion of the population still allows data sharing for targeted advertising. There may be increasing awareness of digital privacy, but many people still don't take active steps to prevent advertising tracking. People in these countries may trust advertising platforms or believe that the benefits of personalized ads outweigh privacy concerns. While tools to refuse advertising use may be available, some users may not be fully educated on how to use them, or they may not consider the trade-off significant enough.

Poland, Slovenia, and Slovakia have between 30-40% of individuals refusing the use of their personal data for advertising purposes. This indicates a moderate level of privacy awareness, with a larger portion of the population opting out of data collection for advertising. A growing awareness of privacy issues, including the risks of personalized ads, is likely influencing more people in these countries to take control of their personal data. Privacy regulations like GDPR may have had a significant impact, leading to higher engagement with privacy settings.

Countries such as Belgium, Germany, Estonia, Greece, Croatia, Hungary, Italy, Lithuania, Luxembourg, and Malta have between 40-50% of individuals refusing the use of their personal data for advertising purposes. This range suggests a high level of concern about privacy,

where a significant portion of the population is actively managing their data preferences to limit advertising targeting. Countries like Germany and Belgium have a strong tradition of data protection, and the GDPR likely plays a key role in raising awareness and encouraging individuals to take steps to protect their privacy. People in these countries tend to have a higher level of awareness and knowledge about how their data is used, particularly for advertising purposes, and are more likely to use tools to limit its use. Many of these countries have experienced public discussions about data exploitation and surveillance, leading to a greater emphasis on controlling personal data.

Countries like Austria, Cyprus, Czech Republic, France, Portugal, and Sweden have between 50-60% of individuals refusing to allow the use of their personal data for advertising. This demonstrates a very high level of privacy awareness, where more than half of the population in these countries is actively managing their data preferences and refusing the use of their personal data for advertising. The implementation of GDPR across Europe has significantly increased awareness and made it easier for individuals to opt out of data collection for targeted ads. These countries have high digital literacy, meaning people are well-versed in the tools available to limit advertising use and understand the risks associated with online data sharing.

Denmark, Spain, Finland, Ireland, and the Netherlands have more than 60% of individuals refusing the use of their personal data for advertising purposes. This high percentage reflects a very strong privacy culture in these countries, where the majority of people actively refuse targeted advertising based on their personal data. These countries have a very strong emphasis on privacy rights, and people are well-educated about how to manage their data preferences. There is likely a cultural emphasis on individual privacy and data protection, with citizens trusting privacy tools and feeling empowered to control the use of their data for commercial purposes.

2.7.Percentage of individuals that manage access to personal data on the internet (3 months): checked that the website where personal data provided was secure in 2023

Bulgaria has fewer than 6% of individuals checking whether a website is secure before providing personal data. This suggests a very low level of awareness or concern about website security when it comes to personal data protection in this country. Many people may not understand the risks associated with providing personal data to unsecured websites or may not know how to verify a website’s security. Limited understanding of basic security measures, such as recognizing secure website URLs (with HTTPS) or identifying secure connections, may contribute to this low percentage.

Romania (6.78%) falls into the 6-16% range, indicating a slightly lower percentage of individuals who check the security of a website before providing personal data. However, this still suggests a relatively low level of engagement with online security practices. Users may assume

Table 7 Percentage of individuals that manage access to personal data on the internet (3 months): checked that the website where personal data provided was secure in 2023

% of individuals 2.7.	Countries	No of countries
less than 6	BG	1
6-16	RO	1
16-26	BE, CY, DE, EL, IT, LT, LV, PL, SI, SK	10
26-36	HR, HU, LU, SE	4
36-46	AT, CZ, EE, FR, IE	5
more than 46	DK, ES, FI, MT, NL, PT	6
Total		27

that local or familiar websites are secure and may not think to check the security of unfamiliar sites. Digital literacy might still be developing, with people not fully educated about how to check for website security before sharing personal information.

Belgium, Cyprus, Germany, Greece, Italy, Lithuania, Latvia, Poland, Slovenia, and Slovakia have between 16-26% of individuals checking the security of websites before providing personal data. This suggests a moderate awareness of online security practices in these countries. While the level of security checks is still relatively low, these countries likely have higher digital literacy than those with fewer checks, and individuals are starting to realize the importance of ensuring a website is secure. In countries like Germany (which has strong privacy laws like GDPR), there may be greater awareness of security measures required before sharing personal data online.

Croatia, Hungary, Luxembourg, and Sweden fall into this range, where 26-36% of individuals check whether a website is secure before submitting their personal data. This represents a higher level of awareness and caution about website security. In countries like Sweden, where there is a high level of digital literacy and a strong focus on privacy, individuals are more likely to be cautious about where and how they share personal

data. These countries may have stronger digital education systems that teach individuals how to identify secure websites (e.g., recognizing HTTPS and security certificates). Governments and companies in these countries may provide more robust resources and campaigns that help people understand the importance of checking website security.

Austria, Czech Republic, Estonia, France, and Ireland have between 36-46% of individuals checking the security of websites before providing personal data. This reflects a relatively high level of caution and digital awareness. GDPR and other data protection laws have likely influenced individuals in these countries to be more cautious with their personal data, encouraging the practice of checking website security. Countries like Estonia and Ireland have a high level of digital engagement and education, where individuals are likely well-informed about the risks of unsecured websites.

Denmark, Spain, Finland, Malta, the Netherlands, and Portugal have more than 46% of individuals checking whether websites are secure before submitting their personal data. These countries demonstrate a very high level of awareness and concern about online security. Countries like Finland and Denmark are leaders in digital literacy and have strong educational programs focused on online security and privacy, resulting

in more individuals checking website security. GDPR and other national data protection laws have contributed to a high level of data protection awareness, encouraging individuals to take responsibility for their online security.

2.8. Percentage of individuals that manage access to personal data on the internet (3 months): at least one of I_MAPS_RPS [1], I_MAPS_RRGL [2], I_MAPS_LAP [3], I_MAPS_RAAD [4], I_MAPS_CWSC [5] in 2023

Table 8 Percentage of individuals that manage access to personal data on the internet (3 months): at least one of I_MAPS_RPS, I_MAPS_RRGL, I_MAPS_LAP, I_MAPS_RAAD, I_MAPS_CWSC in 2023

% of individuals 2.8.	Countries	No of countries
less than 47	RO	1
47-55	BG, LV, PL, SI	4
55-63	HR, IT, LT, SK	4
63-71	BE, CY, DE, FR, LU, EL	6
71-79	AT, EE, ES, HU, MT, PT, SE	7
more than 79	NL, CZ, DK, FI, IE	5
Total		27

The data refers to various privacy management actions that individuals take to control access to their personal data on the internet over a three-month period. Each of the measures outlined in the provided variables – [1] through [5] – reflects a different aspect of how individuals are actively managing their online privacy.

2.8.1. Reading Privacy Policy Statements Before Providing Personal Data (I_MAPS_RPS)

This measure refers to individuals who have actively read the privacy policy statements of websites or services before sharing personal data. This is one of the most basic yet effective ways to understand how a website or service intends to use your personal data. It gives individuals insight into whether their data will be shared with third parties, retained, or used for specific

purposes like advertising or profiling. Engaging in this behavior shows a high level of privacy awareness, as users are making informed decisions about their data. However, many individuals may still avoid reading privacy policies due to the length, complexity, or lack of clarity in many policies.

2.8.2. Restricting or Refusing Access to Geographical Location (I_MAPS_RRGL)

This measure indicates that individuals have restricted or refused access to their geographical location while using websites or applications. Many websites and apps ask for access to a user's location for a variety of reasons, such as personalized content or advertisements. By restricting or refusing access, individuals protect their location privacy and prevent unnecessary data collection.

2.8.3. Limiting Access to Profile or Content on Social Networking Sites or Shared Online Storage (I_MAPS_LAP)

This refers to individuals who have limited access to their profiles or shared content on social media platforms or cloud storage services. Limiting who can see certain posts, profiles, or content on social networking sites or shared online storage is crucial for managing one's digital footprint. Restricting access helps ensure that only trusted individuals or groups can view sensitive or personal information. By limiting access, users prevent unauthorized access to personal content, which can help avoid data breaches or exploitation. Social media platforms can often be overly permissive with privacy settings, so users who adjust these settings

are taking an important step in safeguarding their online identity.

2.8.4. Refusing Allowing the Use of Personal Data for Advertising Purposes (I_MAPS_RAAD)

This measure reflects individuals who have refused to allow websites or services to use their personal data for targeted advertising purposes that can often be sold to third parties or used to build extensive personal profiles. Refusing permission to use personal data for ads can reduce unwanted data tracking, prevent targeted ads, and help protect personal privacy. Individuals who take this step actively protect themselves from invasive marketing techniques. It's a clear indication of a user's desire to preserve privacy and limit how companies use their data. The more people who opt-out, the more pressure it puts on companies to offer transparent, privacy-respecting practices.

2.8.5. Checking Whether the Website Where Personal Data Was Provided Was Secure (I_MAPS_CWSC)

This measure indicates whether individuals have checked whether the website they provided personal data to is secure, such as verifying if the site uses HTTPS, a safety logo, or a security certificate. Ensuring website security before

sharing personal data helps protect against identity theft, fraud, and other cyber threats. Individuals who take this step demonstrate a strong understanding of online security and are taking proactive measures to protect their personal information from cybercriminals.

Romania (46.28%) is the only country in this range, where less than 47% of individuals engage in at least one of the privacy management actions. There may be limited awareness or understanding of online privacy issues, with many users not fully aware of the available privacy settings. Or the population may have lower levels of digital literacy when it comes to managing privacy online. People may not prioritize privacy management or may trust websites and online services to a higher degree, resulting in less effort to manage personal data.

Bulgaria, Latvia, Poland, and Slovenia are in the range of 47 – 55%. These countries might be starting to recognize the importance of privacy, influenced by regulations like the GDPR (General Data Protection Regulation), leading to a moderate increase in engagement. People in these countries are becoming more cautious about online privacy, though their engagement is still relatively moderate compared to other regions. Also there may be a rising number of digitally literate individuals in

these countries who are starting to take privacy more seriously, though broader adoption is still in progress.

Between 55-63% are Croatia, Italy, Lithuania, and Slovakia. People in these countries may have higher levels of understanding about the risks of sharing personal information online, motivating them to take steps to protect their privacy. As privacy regulations like the GDPR continue to take effect, individuals in these countries may feel more empowered to manage their personal data and control access to it. Given the widespread use of social media platforms, individuals might be increasingly aware of the importance of managing their profiles and limiting access to personal data on these platforms.

Belgium, Cyprus, Germany, France, Luxembourg, and Greece are in the range of 63-71%. These countries are more likely to have strict data protection laws, such as the GDPR, that help raise awareness about online privacy and compel individuals to take privacy protection seriously. There may be a cultural emphasis on the importance of safeguarding personal data, which could contribute to higher engagement in privacy management activities. These countries may have a more digitally literate population that is better equipped to navigate the complexities of managing online

privacy, leading to a higher adoption of privacy management practices.

Austria, Estonia, Spain, Hungary, Malta, Portugal, Sweden are in the range of 71-79% of individuals that engage in at least one of the privacy management actions. Citizens in these countries are likely to be highly aware of online security and privacy, especially as these countries often have strong digital infrastructures and a highly connected population. The influence of strong data protection laws, such as the GDPR, and national privacy initiatives likely contributes to individuals being proactive about managing their personal data. As data breaches and cyber threats have become more common, individuals in these countries may have developed a heightened awareness of the risks associated with online privacy, motivating them to engage in protective actions.

With more than 79% of individuals that engage in at least one of the privacy management actions are Netherlands, Czech Republic, Denmark, Finland, and Ireland. These countries exhibit the highest level of engagement, possibly due to a well-established culture of privacy protection and strong national regulations that prioritize personal data security. Countries like Denmark, the Netherlands, and Finland have a reputation for robust data protection practices and strong public trust in

privacy laws. This trust likely leads to greater participation in privacy management practices. A high level of digital literacy, along with active campaigns to educate citizens about their privacy rights, likely results in a more privacy-conscious population that takes proactive steps to protect their data.

3. CONCLUSIONS

Trust, security, and privacy are very important today. The internet must be used with great caution, and security measures should be regularly updated.

Concerning the use of browser settings to prevent or limit cookies most European countries are in the mid-range for online privacy interest, but there are clear examples of countries with high interest, such as Finland and the Netherlands. Data protection policies, national regulations, and digital education significantly influence user behavior in this regard.

The varying levels of privacy software adoption to limit tracking across EU countries highlight the differing degrees of awareness, education, and government regulation regarding online privacy. Countries with higher usage rates, such as Belgium, the Netherlands, and the Scandinavian countries, demonstrate a more advanced level of understanding and action

towards data protection. Meanwhile, countries like Bulgaria and Cyprus show that there is still work to be done in terms of raising awareness and improving access to privacy tools. National regulations like the GDPR have had a significant impact on encouraging privacy protection across the EU, but adoption rates still differ due to factors like digital literacy, accessibility of tools, and the general cultural attitudes toward privacy in each country.

The data shows varying levels of awareness and action regarding privacy policies across European countries. While some countries have made significant progress in terms of data protection awareness (e.g., Finland, Austria, Netherlands), others still lag behind, with lower percentages of individuals engaging with privacy policies before sharing personal data (e.g., Belgium, Cyprus). The overall trend reflects a growing awareness of the importance of online privacy, especially in countries with strong digital infrastructure and privacy regulations. However, there is still a significant gap in how different populations engage with privacy policies, which could be influenced by factors such as digital education, trust in online services, and the perceived complexity or inconvenience of reading privacy policies. Countries with a higher percentage of people reading

privacy policies are likely benefiting from stronger privacy regulations, cultural factors, and more accessible information about data rights.

The data reveals a clear trend of increasing privacy awareness and actions related to location tracking across Europe. The countries with higher percentages (e.g., Finland, Netherlands, Denmark) have a strong culture of privacy, with citizens who are well-educated about the risks of sharing geographical data. These countries also tend to have robust privacy laws and regulations, which contribute to a more proactive approach to managing personal information. On the other hand, countries with lower engagement (e.g., Bulgaria, Latvia) may still be in the process of building up their privacy awareness and digital infrastructure. While GDPR has raised awareness about data protection across the EU, cultural and digital literacy factors play a significant role in determining how individuals approach location privacy.

The data indicates a growing trend of individuals across Europe becoming more aware of their digital privacy, particularly regarding social media and online storage platforms. Countries with higher percentages (e.g., Netherlands, Denmark, Finland) have a strong culture of data protection, supported by strong regulations like GDPR and high

levels of digital literacy. Conversely, countries with lower percentages (e.g., Romania, Bulgaria) may have lower levels of privacy awareness and fewer tools available to help individuals manage access to their personal data. In summary, while privacy concerns are on the rise across Europe, there remains a significant gap between countries that have established a strong culture of privacy and those still developing such practices. The increasing implementation of GDPR is likely contributing to higher levels of engagement with privacy tools, but digital literacy and public awareness remain key drivers of behavior in this area.

The data illustrates significant variation across Europe in how individuals manage their personal data, specifically with respect to advertising purposes. The trend is clear: countries with stronger privacy protections, such as those with higher percentages (e.g., Denmark, Netherlands, Germany, Sweden), exhibit a higher level of privacy awareness and proactive management of personal data. The influence of GDPR is evident, as it has played a central role in educating and empowering individuals to refuse the use of their personal data for targeted advertising. Countries with lower percentages (e.g., Bulgaria, Romania) may have lower levels of

digital literacy or less familiarity with privacy tools, contributing to a lower refusal rate. However, across the board, there is an increasing trend of individuals refusing to allow the use of their personal data for advertising purposes, indicating growing privacy concerns and an increasing desire for control over personal information.

The data highlights a strong correlation between digital literacy, privacy regulations, and the percentage of individuals checking website security before providing personal data. Countries with higher percentages, such as Denmark, Finland, and the Netherlands, demonstrate advanced digital literacy and a culture of privacy, with individuals taking more proactive steps to ensure their data is protected. On the other hand, countries with lower percentages, like Bulgaria and Romania, indicate that awareness and education around online security may still be developing. These countries could benefit from increased awareness campaigns and education on how to identify secure websites to protect personal data. Overall, the trend suggests that across Europe, individuals are becoming more conscious of the importance of checking website security before submitting personal data, with countries with higher digital literacy and stronger privacy regulations leading the way.

As regional trends, the countries in Western Europe and Northern Europe tend to have higher engagement in managing personal data privacy. This may be due to more established privacy laws, higher levels of digital literacy, and a cultural emphasis on personal data protection. Concerning the GDPR Influence, the countries in the European Union (EU), particularly those with strong privacy frameworks like the GDPR, are more likely to see high levels of engagement in data privacy measures. The GDPR has significantly impacted individuals' awareness and understanding of their rights over personal data, leading to a higher percentage of people taking active measures to protect their data.

Taking into consideration the growing privacy awareness we can see that while countries like Romania and Bulgaria show lower engagement, privacy awareness is gradually growing across Europe. As digital literacy and awareness rise, we can expect more individuals in these regions to engage with privacy management practices in the future. In conclusion, the data confirms a significant divide in privacy management practices across Europe, with Western and Northern European countries showing the highest levels of engagement. This reflects the importance of regulatory frameworks, digital literacy, and

cultural attitudes toward privacy in shaping how individuals protect their personal data online.

These trends illustrate a significant shift towards increased awareness and control over personal data. Individuals are taking more steps to protect their privacy, from limiting cookies to managing how their data is used for advertising. As privacy concerns continue to grow, it is evident that people are becoming more proactive in managing their online identities, and businesses must adapt to these evolving expectations by offering greater transparency and stronger privacy controls.

ENDNOTES

- [1] I_MAPS_RPS – I have carried out the following to manage access to my personal data on the internet in the last 3 months: Read privacy policy statements before providing personal data.
- [2] I_MAPS_RRGL – I have carried out the following to manage access to my personal data on the internet in the last 3 months: Restricted or refused access to my geographical location.
- [3] I_MAPS_LAP – I have carried out the following to manage access to my personal data on the internet in the last 3 months: Limited access to profile or content on social networking sites or shared online storage.
- [4] I_MAPS_RAAD – I have carried out the following to manage access to my personal data on the internet in the last 3 months: Refused

allowing the use of personal data for advertising purposes.

- [5] I_MAPS_CWSC – I have carried out the following to manage access to my personal data on the internet in the last 3 months: Checked that the website where I provided personal data was secure (e.g. https sites, safety logo or certificate).

REFERENCES

- [1] <https://ec.europa.eu/eurostat/data/database>
- [2] https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm
- [3] https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_ip20/default/table?lang=en&category=isoc.isoc_i.isoc_ci_sci
- [4] https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_sp20/default/table?lang=en&category=isoc.isoc_i.isoc_ci_sci
- [5] https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_prv20/default/table?lang=en&category=isoc.isoc_i.isoc_ci_sci
- [6] https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_acfas/default/table?lang=en&category=isoc.isoc_i.isoc_ci_sci
- [7]***Eurostat, *European compilers' manual for statistics on the use of ICT in households and by individuals*, 2023 edition