The current situation of the personal data protection literacy on european level

BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

Sumary

Figures and table

1. DATA PROTECTION

As of May 2018, with the entry into application of the General Data Protection Regulation, there is one set of data protection rules for all companies operating in the EU, wherever they are based.

Stronger rules on data protection mean:

- People have more control over their personal data.
- Businesses benefit from a level playing field.

1.1. LEGAL FRAMEWORK

The legal reference is "Regulation (EU) 2018/1725" of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data", repealing Regulation (EC) 45/2001 and Decision No 1247/2002/EC.

On 1 February 2012 the ECA adopted implementing rules pursuant to Regulation (EC) 45/2001 (cf. Decision No. 11/2012 of 01/02/2012).

Other references relevant in the context of the protection of privacy are:

- The Treaty on European Union
- The EU Charter of Fundamental Rights The European Union recognises the rights, freedoms and principles set out in the charter, granting a specific right to personal data protection for the first time.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – "GDPR") on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
- Communication from the Commision to the European Parliament and the Council Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, repealing Council framework Decision 2008/977/JH.

- Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data" (previous regulation applicable to EU Institutions, Agencies and Bodies).
- 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" (previous directive applicable within the EU before the entry into force of the General Data Protection Regulation (GDPR)).
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
- Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- European Convention for the Protection of Human Rights and Fundamental Freedoms whereas the aim of the Council of Europe is to recognise, maintain and protect human rights and fundamental freedoms such as the right to respect for private life.
- Convention 108 of the Council of Europe Provides safeguards for everyone's rights and fundamental freedoms, in particular the right to respect for privacy, considering the increasing transborder flow of personal data undergoing automatic processing
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
- Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').
- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector replaced by Directive 2002/58/EC.
- Council framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, no longer in force, replaced by Directive (EU) 2016/680.

1.2. ABOUT THE REGULATION AND DATA PROTECTION

1.2.1. Personal data

Personal data is any information that relates to an **identified or identifiable living individual**. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Personal data that has been de-identified, encrypted or **pseudonymised** but can be used to re-identify a person remains personal data and falls within the scope of the law.

Personal data that has been rendered **anonymous** in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

The law protects personal data r**egardless of the technology used for processing that data** – it's technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order). It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.

Examples of personal data:

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone)*;
- an Internet Protocol (IP) address;
- a cookie ID*;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

Examples of data not considered personal data:

* Note that in some cases, there is a specific sectoral legislation regulating for instance the use of location data or the use of cookies – the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (OJ L 201, 31.7.2002, p. 37) and Regulation (EC) No 2006/2004) of the European Parliament and of the Council of 27 October 2004 (OJ L 364, 9.12.2004, p. 1).

- a company registration number;
- an email address such as info@company.com;
- anonymised data.

1.2.2. General Data Protection Regulation (GDPR) govern

Regulation (EU) 2016/679[1], the European Union's ('EU') new General Data Protection Regulation ('GDPR'), regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU.

It doesn't apply to the processing of personal data of deceased persons or of legal entities.

The rules don't apply to data processed by an individual for purely personal reasons or for activities carried out in one's home, provided there is no connection to a professional or commercial activity. When an individual uses personal data outside the personal sphere, for socio-cultural or financial activities, for example, then the data protection law has to be respected.

1.2.3. Data processing

Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

The General Data Protection Regulation (GDPR) applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing, if it is part of a structured filing system.

- examples of processing;
- staff management and payroll administration;
- access to/consultation of a contacts database containing personal data;
- sending promotional emails[2];
- shredding documents containing personal data;
- posting/putting a photo of a person on a website;

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[2] To send direct marketing emails, you also have to comply with the marketing rules set out in the ePrivacy Directive.

- storing IP addresses or MAC addresses;
- video recording (CCTV).

1.2.4. Data protection authorities

DPAs are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against violations of the General Data Protection Regulation and the relevant national laws. There is one in each EU Member State.

Generally speaking, the main contact point for questions on data protection is the DPA in the EU Member State where your company/organisation is based. However, if your company/organisation processes data in different EU Member States or is part of a group of companies established in different EU Member States, that main contact point may be a DPA in another EU Member State.

Find your National Data Protection Authority online.

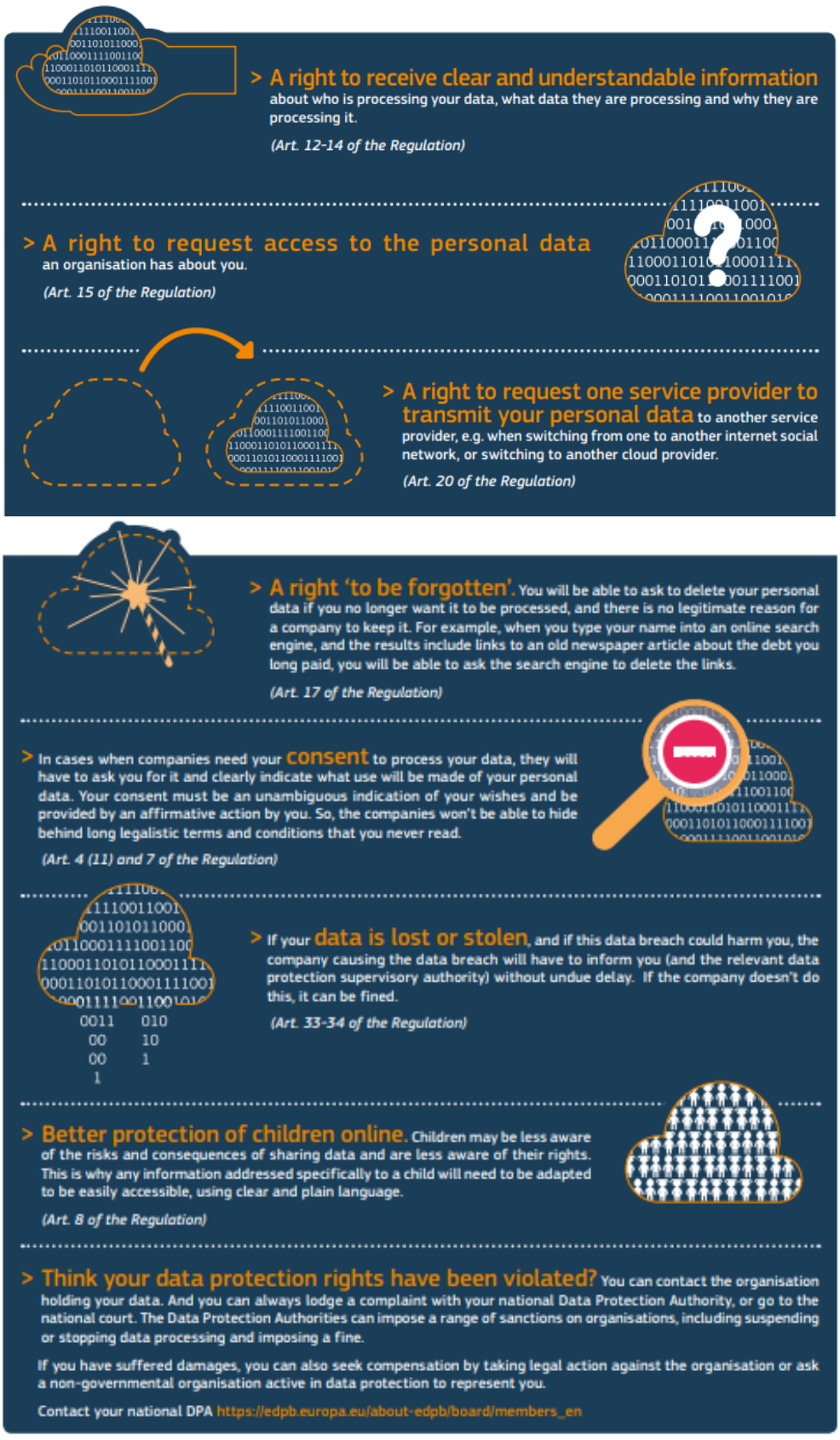
1.3. RIGHTS FOR CITIZENS

1.3.1. What are your rights?

You have the right to:

- **information** about the processing of your personal data;
- **obtain access to** the personal data held about you;
- ask for incorrect, inaccurate or incomplete personal data to be **corrected**;
- request that personal data **be erased** when it's no longer needed or if processing it is unlawful;
- **object** to the processing of your personal data for marketing purposes or on grounds relating to your particular situation;
- request the **restriction** of the processing of your personal data in specific cases;
- receive your personal data in a machine-readable format and send it to another controller (**'data portability'**);
- request that decisions based on **automated processing** concerning you or significantly affecting you and based on your personal data are made by natural persons, not only by computers. You also have the right in this case to express your point of view and to contest the decision.

Figure 1. Rights for citizens



Source: European Commission (2019)

To exercise your rights you should contact the company or organisation processing your personal data, also known as the controller. If the company/organisation has a Data Protection Officer ('DPO') you may address your request to the DPO. The company/organisation must respond to your requests without undue delay and at the latest within 1 month. If the company/organisation doesn't intend to comply with your request they must state the reason why. You may be asked to provide information to confirm your identity (such as, clicking a verification link, entering a username or password) in order to exercise your rights.

These rights apply across the EU, regardless of where the data is processed and where the company is established. These rights also apply when you buy goods and services from non-EU companies operating in the EU.

1.3.2. What information should you receive when you provide your personal data?

When you provide your personal data, you must receive, among other things, information about:

- the name of the company or organisation that is processing your data (including the contact details of the DPO, if there is one);
- the purposes for which the company/organisation will use your data;
- the categories of personal data concerned;
- the legal basis for processing your personal data;
- the length of time for which your data will be stored;
- other companies/organisations that will receive your data;
- whether data will be transferred outside the EU;
- your basic rights in the field of data protection (for example, the right to access and transfer data or have it removed);
- the right to lodge a complaint with a Data Protection Authority (DPA);
- the right to withdraw your consent at any time;
- the existence of automated decision-making and the logic involved, including the consequences thereof.

The information should be presented in a concise, transparent, intelligible way and drafted in clear and plain language.

1.3.3. How can you access your personal data held by a company/organisation?

You have a right to ask for and obtain from the company/organisation confirmation as to whether or not it holds any personal data which concerns you.

If they do have your personal data then you have the right to access that data, be provided with a copy and get any relevant additional information (such as their reason for processing your personal data, the categories of personal data used, etc.).

This right of access should be easy and be made possible at reasonable intervals. The company/organisation should provide a copy of your personal data free of charge. Any further copies may be subject to a reasonable fee. When the request is made by electronic means (for example through an e-mail), and unless otherwise requested by you, the information should be provided in a commonly used electronic form.

This right is not absolute: the use of the right to access your personal data should not affect the rights and freedoms of others, including trade secrets or intellectual property.

EXAMPLE

You borrow books from a library. You can ask the library to provide you with the personal data which concerns you that they hold. The library should then provide you with all information about you that is stored by them. For example, when you first started using the library services, which books you have borrowed; whether you have ever had any book overdue and fines you might have incurred.

You subscribed to a loyalty card scheme of a supermarket chain located in different parts of the city and throughout the country. If you use your right to ask for information about and obtain your personal information stored by the loyalty card scheme, you should receive information about, for example, how often you used the card, at which supermarkets you did your shopping, any discounts you were awarded and whether you were targeted through the use of profiling techniques, and in which way, whether the supermarket, which is part of a multinational chain of companies, has disclosed your data to its sister company selling perfumes and cosmetics.

1.3.4. Your data is incorrect, can you correct it?

If you believe that your personal data might be incorrect, incomplete or inaccurate you can ask the company or organisation to correct your data. They must do so without undue delay (in principle within 1 month) or justify in writing why the request cannot be accepted.

EXAMPLE

A credit bureau processes information provided by your former landlord whereby it is stated that you owe him 3 months' rent. You have just won a legal dispute and his claim for the 3 months' rent was ruled to be unfounded. You may ask the credit bureau to correct the data it holds about you so that you aren't put at a disadvantage in the future when credit requests are processed.

1.3.5. Can you ask a company/organisation to send you your personal data so that you can use it somewhere else?

If a company is processing your personal data on the basis of your consent or a contract, you can ask the company to transfer your personal data to you.

You can also ask for your personal data to be transferred directly to another company whose services you would like to use, when it's technically feasible.

EXAMPLE

You are a member of an online social media network. You decide that a new rival social media network is better suited to your aims and age-group. You can ask your current online social media network to transfer your personal data, including your photos, to the new social media network.

1.3.6. Can you ask a company/organisation to stop processing your personal data?

You have the right to object to the processing of your personal data and ask a company/ organisation to stop processing your personal data if is being processed for the purpose of:

- direct marketing;
- scientific/historical research and statistics;
- their own legitimate interest or in carrying out a task in the public interest/for an official authority.

If you object to direct marketing, the company must stop using your personal data and comply with your request without asking for a fee.

However, a company/organisation can continue to process your personal data, despite your objections, if:

- in the case of processing for the purposes of scientific/historical research and statistics, the processing is necessary for the performance of a task carried out for reasons of public interest;
- in the case of processing based on legitimate interests or on the performance of a task in the public interest/exercise of official authority, they can prove that they have compelling legitimate grounds that override your interests, rights and freedoms. Therefore, a balancing exercise is required.

The company should inform you of your right to object when they first make contact with you.

EXAMPLE

You bought two tickets to see your favourite band play live through an online ticketing company. Afterwards, you are bombarded with adverts for concerts and events that you're not interested in. You inform the online ticketing service company that you don't want to receive further advertising material. The company should stop processing your personal data for direct marketing and, shortly afterwards, you should no longer receive emails from them. They shouldn't charge you for this.

1.3.7. Can you ask a company to delete your personal data?

Yes, you can ask for your personal data to be deleted when, for example, the data the company holds on you is no longer needed or when your data has been used unlawfully. Personal data provided when you were a child can be deleted at any time.

This right also applies **online** and is often referred to as the **'right to be forgotten'**. In specific circumstances, you may ask companies that have made your personal data available online to delete it. Those companies are also obliged to take reasonable steps to inform other companies (controllers) that are processing the personal data that the data subject has requested the erasure of any links to, or copies of, that personal data.

It's worth keeping in mind that this right is not an absolute right, meaning that other rights, such as the freedom of expression and scientific research, are also safeguarded.

EXAMPLES

Data should be deleted

You have joined a social networking site. After a while, you decide to leave the networking site. You have the right to ask the company to delete the personal data belonging to you.

Data can't immediately be deleted

A new bank offers good home loan deals. You're buying a new house and decide to switch to the new bank. You ask the 'old' bank to close down all accounts and request to have all your personal details deleted. The old bank, however, is subject to a law obliging banks to store all customer details for 10 years. The old bank can't simply delete your personal details. In this case, you may want to ask for restriction of processing of your personal data. The bank may then only store the data for the period of time required by law and can't perform any other processing operations on them.

Data should be deleted

When you do an online search using your name and surname the results show a link to a newspaper article. The information in the newspaper dates back a number of years and is related to an issue – a real-estate auction connected with debt recovery proceedings – settled a long time ago that is now irrelevant. If you are not a public figure and your interest in having the article removed outweighs the general public's interest in having access to the information then the search engine is obliged to remove links to web pages including your name and surname from the results.

1.3.8. When should you exercise your right to restriction of processing of your personal data?

Generally speaking, in cases where it's unclear whether and when personal data will have to be deleted, you may exercise your right to restriction of processing. That right can be exercised when:

- the accuracy of the data in question is contested;
- you don't want the data to be erased;
- the data is no longer needed for the original purpose but may not be deleted yet because of legal grounds;
- the decision on your objection to processing is pending.

'Restriction' means that your personal data may, with the exception of storage, only be processed with your consent for the establishment, exercise or defence of legal claims, for the protection of the rights of another natural or legal person or for reasons of public interest of the EU or of an EU Member State. You must be informed before the restriction is lifted.

EXAMPLE

A new bank on the domestic market offers good home loan deals. You are buying a new house and so decide to switch banks. You ask the 'old' bank to close down all accounts and request to have all your personal details deleted. The old bank, however, is subject to a law obliging banks to store all customer details for 10 years. The old bank is legally obliged to store your data but you can still ask for restriction of the data to make sure that it's not accidentally used for unwanted purposes.

1.3.9. Can you be subject to automated individual decision-making, including profiling?

Profiling is done when your personal aspects are being evaluated in order to make predictions about you, even if no decision is taken. For example, if a company or organisation assesses your characteristics (such as your age, sex, height) or classifies you in a category, this means you are being profiled.

Decision-making based solely on automated means happens when decisions are taken about you by technological means and without any human involvement. They can be taken even without profiling.

The data protection law establishes that you have the right not to be subject to a decision based solely on automated means, if the decision produces legal effects concerning you or significantly affects you in a similar way. A decision produces legal effects when your legal rights are impacted (such as your right to vote). In addition, processing can significantly affect you if it influences your circumstances, behaviour or choices. For example, automatic processing may lead to the refusal of your online credit application.

Profiling and automated decision-making are common practice in a number of sectors, such as banking and finance, taxation and healthcare. It can be more efficient, but may be less transparent and may restrict your choice.

Although, as a general rule, you may not be the subject of a decision based solely on automated processing, this type of decision-making may exceptionally be allowed if the use of algorithms is allowed by law and suitable safeguards are provided.

Decisions based solely on automated means are also allowed where:

- the decision is necessary that is to say, there must be no other way to achieve the same goal to enter or perform a contract with you;
- you have given your explicit consent.

In both instances, the decision taken needs to protect your rights and freedoms, by implementing suitable safeguards. The company or organisation must, at least, inform you of your right to human intervention and to make the required procedural arrangements. Furthermore, the company or organisation should allow you to express your point of view and inform you that you may contest the decision.

Algorithm-based decisions may not make use of special categories of data, unless you have given your consent or the processing is allowed by EU or national law.

EXAMPLE

You use an online bank for a loan. You are asked to insert your data and the bank's algorithm tells you whether the bank will grant you the loan or not and gives the suggested interest rate. You must be informed that you may express your opinion, contest the decision and demand that the decision made via the algorithm be reviewed by a person.

1.3.10. Can personal data about children be collected?

Additional protection is granted to this type of personal data since children are less aware of the risks and consequences of sharing data and of their rights. Any information addressed specifically to a child should be adapted to be easily accessible, using clear and plain language.

For most online services the consent of the parent or guardian is required in order to process a child's personal data on the grounds of consent up to a certain age. This applies to social networking sites as well as to platforms for downloading music and buying online games.

The age threshold for obtaining parental consent is established by each EU Member State and can be between 13 and 16 years. Check with your National Data Protection Authority.

Companies have to make reasonable efforts, taking into consideration available technology, to check that the consent given is truly in line with the law. This may involve implementing age-verification measures such as asking a question that an average child would not be able to answer or requesting that the minor provides his parents' email to enable written consent.

Preventive or counselling services offered directly to children are exempted from the requirement for parental consent as they seek to protect a child's best interests.

EXAMPLES

Parental consent required

You have a 12-year-old daughter. She would like to join a popular social media network and is asked for consent to process information about her religion. You would need to give your consent in case you want her to join that social media network.

Parental consent not required

Your 17-year-old son is considering participating in an online survey about his clothes consumption patterns. The website requests consent to process his data. As he is over 16, he can give his consent without asking for yours.

1.3.11. Can your employer require me to give you consent to use your personal data?

The employer-employee situation is generally considered as an imbalanced relationship in which the employer wields more power than the employee. Since consent has to be freely given, and in light of the imbalanced relationship, your employer in most cases can't rely on your consent to use your data.

There might be situations in which processing of an employee's personal data based on the employee's consent is lawful, especially if it's in the interest of the employee. For example, if a company grants benefits to the employee or their family members (e.g. discounts on the company's services), processing of the employee's personal data is allowed and lawful, if informed prior consent was given.

EXAMPLE

Consent not valid

Your employer believes that work productivity needs to be improved. To do this he intends to install CCTV cameras in the corridors and at the entrance to the bathrooms. He asks you to give your consent so that he can monitor your movements and the time spent out of office. Even if you do consent, it would be considered invalid and your employer can't install CCTV based on that consent.

1.3.12. How should your consent be requested?

A consent request needs to be presented in a clear and concise way, using language that is easy to understand, and be clearly distinguishable from other pieces of information such as terms and conditions. The request has to specify what use will be made of your personal data and include contact details of the company processing the data. Consent must be freely given, specific, informed and unambiguous. Informed consent means that you must be given information about the processing of your personal data, including at least:

- the identity of the organisation processing data;
- the purposes for which the data is being processed;
- the type of data that will be processed;
- the possibility to withdraw consent (for example by sending an email to withdraw consent);
- where applicable, the fact that the data will be used solely for automated-based decision-making, including profiling;
- information about whether the consent is related to an international transfer of your data, the possible risks of data transfers to countries outside the EU if those countries are not the subject of a Commission adequacy decision and there are no adequate safeguards.

EXAMPLES

Consent not requested as per terms of the law

You enrol at a music school to take piano classes. The enrolment form contains a long document drafted in small print using highly legal and technical terms, which includes the possibility that the school may pass on your personal details to retailers selling musical instruments. The school is in breach of the law as your consent to receive marketing material (potentially from instrument retailers) was not requested as stipulated by law.

You're opening a bank account online and want to confirm your request. You are shown a page with two tick boxes saying 'I accept the terms and conditions' and 'I agree that the decision whether I am entitled to a credit card is solely based upon profiling without any human intervention'. Both tick boxes are activated (checked) by default. You have to deactivate the tick box if you don't want to be subject to a decision on whether you are entitled to a credit card based solely on profiling. Even if you don't deactivate the tick box, the bank would not have obtained valid consent as pre-ticked boxes are not considered to be valid consent under GDPR.

1.3.13. What happens if data you have shared is leaked?

A personal data breach occurs when there's a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data processed. If this happens, the organisation holding the personal data must notify the supervisory authority without undue delay. If the personal data breach is likely to result in a high risk to your rights and freedoms and the risk hasn't been mitigated, then you, as an individual, must also be informed.

Example

You booked your taxi via an online application. The taxi company has suffered a massive personal data breach and driver and user data has been stolen. It appears that no specific security measure was in place to protect the personal data. The company should have informed you about the breach. In this case, you can file a complaint against the taxi company before the national Data Protection Authority ('DPA').

1.3.14. What should you do if you think that my personal data protection rights haven't been respected?

If you think your data protection rights have been breached, you have three options:

- lodge a complaint with your national Data Protection Authority (DPA)

  The authority investigates and informs you of the progress or outcome of your complaint within 3 months;

- take legal action against the company or organisation

  File an action directly in court against a company/organisation if you believe that it has violated your data protection rights. This doesn't stop you lodging a complaint with the national DPA if you so wish;

- take legal action against the DPA

  If you believe that the DPA has not handled your complaint correctly or if you aren't satisfied with its reply or if it doesn't inform you with regard to the progress or outcome within 3 months from the day you lodged your complaint, you can bring an action directly before a court against the DPA.

Sometimes, the company against which the complaint has been lodged processes data in different EU Member States. In this particular case, the competent DPA handles the complaint in cooperation with the DPAs based in the other EU Member States. This system, called the 'one-stop-shop mechanism', ensures complaints are handled more efficiently. For example, it may help connect your complaint with similar complaints lodged in other EU Member States. The DPA where you have lodged the complaint is your main contact point.

Example

You enjoy running. You have bought a watch which calculates your heart rate and speed per kilometre, tracks your route and gathers other relevant data. You upload all your data on the website. You realise that your data has been mixed up with someone else's. You can file a complaint before your DPA against the website.

1.3.15. Can a non-governmental organisation (NGO) make claims on your behalf?

You have the right to mandate an NGO to lodge a complaint on your behalf when the following conditions are fulfilled:

1. the NGO is constituted in accordance with the law;
2. the NGO pursues a public interest objective (for example improving citizens' life in the consumer area);
3. the NGO is active in the area of data protection.

The complaint can be filed both before the relevant Data Protection Authority and also, if the case arises, before a judicial authority. In certain EU Member States, national legislation allows an NGO to lodge a complaint without your mandate.

1.3.16. Can you claim compensation?

You can claim compensation if a company or organisation hasn't respected the data protection law and you've suffered material damages (for example financial loss) or non-material damages (for example distress or loss of reputation). You can make a claim to the company or organisation concerned or before the national courts. You can claim compensation before the courts of the EU Member State where the controller or processor is established. Alternatively, such proceedings may be brought before the courts of the EU Member State of your habitual residence.

EXAMPLE

You place an order on a website. The site suffers a cyber-attack because it doesn't have adequate security. Your credit card details have been put on another website and used to buy items you never ordered. You can claim compensation from the website for the financial damage as they have breached the data protection law by not providing adequate security when processing data.

1.4. RULES FOR BUSINESS AND ORGANISATIONS

1.4.1. Who does the data protection law apply to?

The law applies to:

- a company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; or
- a company established outside the EU offering goods/services (paid or for free) or monitoring the behaviour of individuals in the EU.

If your company is a small and medium-sized enterprise ('SME') that processes personal data as described above you have to comply with the GDPR. However, if processing personal data isn't a core part of your business and your activity doesn't create risks for individuals, then some obligations of the GDPR will not apply to you (for example the appointment of a Data Protection Officer ('DPO')). Note that 'core activities' should include activities where the processing of data forms an inextricable part of the controller's or processor's activities.

EXAMPLES

When the regulation applies

Your company is a small, tertiary education company operating online with an establishment based outside the EU. It targets mainly Spanish and Portuguese

language universities in the EU. It offers free advice on a number of university courses and students require a username and a password to access your online material. Your company provides the said username and password once the students fill out an enrolment form.

When the regulation does not apply

Your company is service provider based outside the EU. It provides services to customers outside the EU. Its clients can use its services when they travel to other countries, including within the EU. Provided your company doesn't specifically target its services at individuals in the EU, it is not subject to the rules of the GDPR.

1.4.2. Do the rules apply to SMEs?

Yes, the application of the data protection regulation depends not on the size of your company/organisation but on the nature of your activities. Activities that present high risks for the individuals' rights and freedoms, whether they are carried out by an SME or by a large corporation, trigger the application of more stringent rules. However, some of the obligations of the GDPR may not apply to all SMEs.

For instance, companies with fewer than 250 employees don't need to keep records of their processing activities unless processing of personal data is a regular activity, poses a threat to individuals' rights and freedoms, or concerns sensitive data or criminal records.

Similarly, SMEs will only have to appoint a Data Protection Officer if processing is their main business and it poses specific threats to the individuals' rights and freedoms (such as monitoring of individuals or processing of sensitive data or criminal records) in particular because it's done on a large scale.

1.4.3. Do the data protection rules apply to data about a company?

No, the rules only apply to personal data about individuals, they don't govern data about companies or any other legal entities. However, information in relation to one-person companies may constitute personal data where it allows the identification of a natural person. The rules also apply to all personal data relating to natural persons in the course of a professional activity, such as the employees of a company/organisation, business email addresses like 'forename.surname@company.eu' or employees' business telephone numbers.

1.4.4. What data can you process and under which conditions?

The type and amount of personal data you may process depends on the reason you're processing it (legal reason used) and what you want to do with it. You must respect several key rules, including:

- personal data must be processed in a lawful and transparent manner, ensuring fairness towards the individuals whose personal data you're processing ('lawfulness, fairness and transparency').
- you must have specific purposes for processing the data and you must indicate those purposes to individuals when collecting their personal data. You can't simply collect personal data for undefined purposes ('purpose limitation').
- you must collect and process only the personal data that is necessary to fulfil that purpose ('data minimisation').
- you must ensure the personal data is accurate and up-to-date, having regard to the purposes for which it's processed, and correct it if not ('accuracy').
- you can't further use the personal data for other purposes that aren't compatible with the original purpose of collection.
- you must ensure that personal data is stored for no longer than necessary for the purposes for which it was collected ('storage limitation').
- you must install appropriate technical and organisational safeguards that ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technology ('integrity and confidentiality').

EXAMPLE

You run a travel agency. When you obtain your clients' personal data, you should explain in clear and plain language why you need the data, how you'll be using it, and how long you intend to keep it. The processing should be tailored in a way that respects the key data protection principles.

1.4.5. Can data be processed for any purpose?

No. The purpose for processing of personal data must be known and the individuals whose data you're processing must be informed. It is not possible to simply indicate that personal data will be collected and processed. This is known as the 'purpose limitation' principle.

1.4.6. Can you use data for another purpose?

Yes, but only in some cases. If your company/organisation has collected data on the basis of legitimate interest, a contract or vital interests it can be used for another purpose but only after checking that the new purpose is compatible with the original purpose.

The following points should be considered:

- the link between the original purpose and the new/upcoming purpose;
- the context in which the data was collected (what is the relationship between your company/organisation and the individual?);
- the type and nature of the data (is it sensitive?);
- the possible consequences of the intended further processing (how will it impact the individual?);
- the existence of appropriate safeguards (such as encryption or pseudonymisation).

If your company/organisation wants to use the data for statistics or for scientific research it is not necessary to run the compatibility test.

If your company/organisation has collected the data on the basis of consent or following a legal requirement, no further processing beyond what is covered by the original consent or the provisions of the law is possible. Further processing would require obtaining new consent or a new legal basis.

EXAMPLES

Further processing is possible

A bank has a contract with a client to provide the client with a bank account and a personal loan. At the end of the first year the bank uses the client's personal data to check whether they are eligible for a better type of loan and a savings scheme. It informs the client. The bank can process the data of the client again as the new purposes are compatible with the initial purposes.

Further processing isn't possible

The same bank wants to share the client's data with insurance firms, based on the same contract for a bank account and personal loan. That processing isn't permitted without the explicit consent of the client as the purpose isn't compatible with the original purpose for which the data was processed.

1.4.7. How much data can be collected?

Personal data should only be processed where it isn't reasonably feasible to carry out the processing in another manner. Where possible, it is preferable to use anonymous data. Where personal data is needed, it should be adequate, relevant, and limited to what is necessary for the purpose ('data minimisation'). It's your company/organisation's responsibility as controller to assess how much data is needed and ensure that irrelevant data isn't collected.

EXAMPLE

Your company/organisation offers car-sharing services to individuals. For those services it may require the name, address and credit card number of your customers and potentially even information on whether the person has a disability (so health data), but not their racial origin.

1.4.8. For how long can data be kept and is it necessary to update it?

You must store data for the shortest time possible. That period should take into account the reasons why your company/organisation needs to process the data, as well as any legal obligations to keep the data for a fixed period of time (for example national labour, tax or anti-fraud laws requiring you to keep personal data about your employees for a defined period, product warranty duration, etc.).

Your company/organisation should establish time limits to erase or review the data stored.

By way of an exception, personal data may be kept for a longer period for archiving purposes in the public interest or for reasons of scientific or historical research, provided that appropriate technical and organisational measures are put in place (such as anonymisation, encryption, etc.).

Your company/organisation must also ensure that the data held is accurate and kept up-to-date.

EXAMPLE

Data kept for too long without an update

Your company/organisation runs a recruitment office and for that purpose it collects CVs of persons seeking employment and who, in exchange for your intermediary services, pay you a fee. You plan to keep the data for 20 years and you take no measures for updating the CVs. The storage period doesn't seem proportionate to the purpose of finding employment for a person in the short to medium term. Moreover, the fact you don't request updates to CVs at regular intervals renders some of the searches useless for the person seeking employment after a certain amount of time (for instance because that person has gained new qualifications).

1.4.9. What information must be given to individuals whose data is collected?

At the time of collecting their data, people must be informed clea rly about at least:

- who your company/organisation is (your contact details, and those of your DPO if any);
- why your company/organisation will be using their personal data (purposes);
- the categories of personal data concerned;
- the legal justification for processing their data;
- for how long the data will be kept;
- who else might receive it;
- whether their personal data will be transferred to a recipient outside the EU;
- that they have a right to a copy of the data (right to access personal data) and other basic rights in the field of data protection (see complete list of rights);
- their right to lodge a complaint with a Data Protection Authority (DPA);
- their right to withdraw consent at any time;
- where applicable, the existence of automated decision-making and the logic involved, including the consequences thereof.

The information may be provided in writing, orally at the request of the individual when identity of that person is proven by other means, or by electronic means where appropriate. Your company/organisation must do that in a concise, transparent, intelligible and easily accessible way, in clear and plain language and free of charge.

When data is obtained from another company/organisation, your company/organisation should provide the information listed above to the person concerned at the latest within 1 month after your company obtained the personal data; or, in case your company/ organisation communicates with the individual, when the data is used to communicate with them; or, if a disclosure to another company is envisaged, when the personal data was first disclosed.

Your company/organisation is also required to inform the individual of the categories of data and the source from which it was obtained including if it was obtained from publicly accessible sources. Under specific circumstances listed in Articles 13(4) and 14(5) of the GDPR your company/organisation may be exempted from the obligation to inform the individual. Please check whether that exemption applies to your company/organisation.

1.4.10. Sensitive data

The following personal data is considered ‘sensitive’ and is subject to specific processing conditions:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- trade-union membership;
- genetic data, biometric data processed solely to identify a human being;

- health-related data;
- data concerning a person's sex life or sexual orientation.

Your company/organisation can only process sensitive data if one of the following conditions is met:

- the explicit consent of the individual was obtained (a law may rule out this option in certain cases);
- an EU or national law or a collective agreement, requires your company/organisation to process the data to comply with its obligations and rights, and those of the individuals, in the fields of employment, social security and social protection law;
- the vital interests of the person, or of a person physically or legally incapable of giving consent, are at stake;
- you are a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim, processing data about its members or about people in regular contact with the organisation;
- the personal data was manifestly made public by the individual;
- the data is required for the establishment, exercise or defence of legal claims;
- the data is processed for reasons of substantial public interest on the basis of EU or national law;
- the data is processed for the purposes of preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of EU or national law, or on the basis of a contract as a health professional;
- the data is processed for reasons of public interest in the field of public health on the basis of EU or national law;
- the data is processed for archiving, scientific or historical research purposes or statistical purposes on the basis of EU or national law.

Further conditions may be imposed by national law on the processing of genetic data, biometric data or data concerning health. Check with your National Data Protection Authority.

EXAMPLES

You can process sensitive data

A doctor sees a number of patients at his clinic. He logs the visit in a database that includes fields such as name/surname of patient, description of symptoms and medication prescribed. That is considered to be sensitive data. The processing of health data by the clinic is allowed under the data protection law because it is required to treat the person and is carried out under the responsibility of a doctor who is subject to an obligation of professional secrecy.

You can't process sensitive data

Your company sells dresses online. In order to tailor the services to the specific interests of your clients, you ask them to provide you with information about sizes, preferred colour, payment method, name and the address so that the product can be delivered. In addition your company asks for your clients' political views. You need the majority of the information to fulfil your side of the contract. However, clients' political views are not a requirement to make and deliver their dresses. Your company cannot ask for that information under that contract.

1.4.11. Are there any specific safeguards for data about children?

Your company/organisation can only process a child's personal data on grounds of consent with the explicit consent of their parent or guardian up to a certain age. The age threshold for obtaining parental consent varies between 13 and 16 years, depending on the age established in each EU Member State. Check with your National Data Protection Authority.

A reasonable effort must be made, taking into consideration available technology, to verify that the consent given is truly in line with the law. That means that your company/organisation must implement age-verification measures (for example control questions, actions on the website).

The consent from the parent or guardian must be obtained if your organisation works on online social networking sites that provide free games to children or family insurance, for example.

If your organisation targets children, you must ensure that any information and communication addressed to a child is easily accessible and in clear and plain language that a child can easily understand.

Preventive or counselling services offered directly to a child don't require parental authorisation since they are aimed at protecting the children's best interests.

1.4.12. Can data received from a third party be used for marketing?

Before acquiring a contact list or a database with contact details of individuals from another organisation, that organisation must be able to demonstrate that the data was obtained in compliance with the General Data Protection Regulation and that it may use it for advertising purposes. For example, if the organisation acquired it based on consent, the consent should've included the possibility to transmit the data to other recipients for their own direct marketing.

Your company/organisation must also ensure that the list or database is up-to-date and that you don't send advertising to individuals who objected to the processing of their personal data for direct

marketing purposes. Your company/organisation must also ensure that if it uses communication tools, such as email, for the purposes of direct marketing, it complies with the rules set out in the ePrivacy Directive (Directive 2002/58/EC1).

Such lists are processed on grounds of legitimate interests and individuals will have a right to object to such processing. Your company/organisation must also inform individuals, at the latest at the time of the first communication with them, that you've collected their personal data and that you'll be processing it for sending them adverts.

EXAMPLE

Two friends, Mrs. A and Mr. B, run, respectively, a gym and a book shop. Each collects data from their respective customers. Mr. B's book shop isn't doing well. His client database has few entries and not many people walk into his shop. He tells Mrs. A that he has a new biography of a famous athlete and asks whether Mrs. A's clients would be interested in receiving advertising about the book. The terms of Mrs. A's privacy notice informed her clients that she could share the data with partners offering products in the health and fitness area. As far as specific consent was given for the purpose of transmitting the data to other recipients for their own direct marketing, Mrs. A can send the client list to Mr. B. No data can be sent about an individual who objected to the processing of their personal data.

1.4.13. What is a data controller or a data processor?

The data controller determines the purposes for which and the means by which personal data is processed. So, if your company/organisation decides 'why' and 'how' the personal data should be processed it is the data controller. Employees processing personal data within your organisation do so to fulfil your tasks as data controller.

Your company/organisation is a joint controller when together with one or more organisations it jointly determines 'why' and 'how' personal data should be processed. Joint controllers must enter into an arrangement setting out their respective responsibilities for complying with the GDPR rules. The main aspects of the arrangement must be communicated to the individuals whose data is being processed.

The data processor processes personal data only on behalf of the controller. The data processor is usually a third party external to the company. However, in the case of groups of undertakings, one undertaking may act as processor for another undertaking.

The duties of the processor towards the controller must be specified in a contract or another legal act. For example, the contract must indicate what happens to the personal data once the contract is terminated. A typical activity of processors is offering IT solutions, including cloud storage.

The data processor may only sub-contract a part of its task to another processor or appoint a joint processor when it has received prior written authorisation from the data controller.

There are situations where an entity can be a data controller, or a data processor, or both.

EXAMPLES

Controller and processor

A brewery has many employees. It signs a contract with a payroll company to pay the wages. The brewery tells the payroll company when the wages should be paid, when an employee leaves or has a pay rise, and provides all other details for the salary slip and payment. The payroll company provides the IT system and stores the employees' data. The brewery is the data controller and the payroll company is the data processor.

Joint controllers

Your company/organisation offers babysitting services via an online platform. At the same time your company/organisation has a contract with another company allowing you to offer value-added services. Those services include the possibility for parents not only to choose the babysitter but also to rent games and DVDs that the babysitter can bring. Both companies are involved in the technical set-up of the website. In that case, the two companies have decided to use the platform for both purposes (babysitting services and DVD/games rental) and will very often share clients' names. Therefore, the two companies are joint controllers because not only do they agree to offer the possibility of 'combined services' but they also design and use a common platform.

1.4.14. Can someone else process the data on my organisation's behalf?

Someone else (a natural or legal person or any other body) may process personal data on your behalf provided there is a contract or other legal act. It is important that the processor you appoint provides sufficient guarantees to implement appropriate technical and organisational measures to ensure that the processing will meet the standards of the General Data Protection Regulation (GDPR) and to guarantee the protection of the rights of the individuals.

The appointed processor can't subsequently appoint another processor without your prior, specific or general written authorisation. The contract or legal act between your company/organisation and the processor should include the following elements:

- the processing can take place only on documented instructions from the controller;

- the processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- the processor must offer a minimal security level defined by the controller;
- the processor must assist in ensuring compliance with the GDPR.

EXAMPLE

A construction company is using a sub-contractor for specific construction work, and provides it with the contact details of the clients where the construction work needs to be done. The sub-contractor further uses the data to send the clients marketing material. The sub-contractor in that case doesn't qualify merely as a 'processor' under the GDPR as the sub-contractor is not only processing personal data on behalf of the construction company, but also further processing it for its own purposes. The sub-contractor is therefore acting as a 'data controller'.

You're a retail company that decides to store a back-up version of your client database on a cloud server. To that end you enter into a contract with a cloud provider known for its data protection standards and which also has a certified system of encryption of data. The cloud provider is your processor as by storing the personal data of your clients in its servers it will be processing personal data on your behalf.

1.4.15. Are the obligations the same regardless of the amount of data your company/ organisation handles?

The General Data Protection Regulation (GDPR) is based on the risk-based approach. In other words, companies/organisations processing personal data are encouraged to implement protective measures corresponding to the level of risk of their data processing activities. Therefore, the obligations on a company processing a lot of data are more onerous than on a company processing a small amount of data.

For example, the probability of hiring a data protection officer for a company/ organisation processing a lot of data is higher than for a company/organisation processing a small amount of data (in that case this links to the notion of processing of personal data on a 'large scale'). At the same time, the nature of the personal data and the impact of the envisaged processing also play a role. Processing of a small amount of data, but which is of a sensitive nature, for example health data, would require implementing more stringent measures to comply with the GDPR.

In all cases, the principles of data protection must be respected and individuals allowed to exercise their rights.

1.4.16. What does data protection 'by design' and 'by default' mean?

Companies/organisations are encouraged to implement technical and organisational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles right from the start ('data protection by design'). By default, companies/organisations should ensure that personal data is processed with the highest privacy protection (for example only the data necessary should be processed, short storage period, limited accessibility) so that by default personal data isn't made accessible to an indefinite number of persons ('data protection by default').

EXAMPLES

Data protection by design

The use of pseudonymisation (replacing personally identifiable material with artificial identifiers) and encryption (encoding messages so only those authorised can read them).

Data protection by default

A social media platform should be encouraged to set users' profile settings in the most privacy-friendly setting by, for example, limiting from the start the accessibility of the users' profile so that it isn't accessible by default to an indefinite number of persons.

1.5. MYTHS ABOUT GENERAL DATA PROTECTION REGULATION

1.5.1. Myth 1: GDPR completely changes the way organisations need to handle their data

The GDPR is not a completely brand-new set of EU data protection rules. It's an evolution of the existing set of rules, based on the strong data protection principles set out in the Data Protection Directive. These rules have been around since 1995, so it's time to make sure that they're fit for the digital age.

1.5.2. Myth 2: GDPR will stifle European innovation in the field of artificial intelligence (AI)

The protection of personal data is a fundamental right in the EU. As such it applies also to processing of personal data through artificial intelligence and robotics. However, when the data used for AI are anonymised, then the requirements of the GDPR do not apply. GDPR has been designed to be technologically neutral and provides the framework for the development of an AI

respectful of citizens. GDPR allows automated decision making where there is a justification either by a contract, explicit consent or a law, and provided that specific safeguards for the individuals concerned are applied, such as the right to receive meaningful information about the logic involved and the envisaged consequences of such processing on them.

1.5.3. Myth 3: Landlords cannot put the names of tenants on the doorbell

The GDPR does not require names to be removed from doorbells or mailboxes. Consent is only one of the legal bases on which data can be processed under the GDPR. Another legal basis applicable in this case is “legitimate interest” as people need to know who lives in a flat in order to contact the person at hand and for distributing mail. If names on doorbells are addressed in the rental contract; the contract as such is another potential legal basis.

1.5.4. Myth 4: GDPR is overwhelming for small businesses

The GDPR is not meant to overburden SMEs. The obligations are calibrated to the size of the business and/or to the nature of the data being processed. Smaller companies, processing less data and not processing sensitive data, such as political views and sexual orientation, will have fewer obligations to follow. For example, not every company has to appoint a Data Protection Officer or carry out a data protection impact assessment.

1.5.5. Myth 5: GDPR makes journalism harder

The new data protection rules take into account the freedom of the press. This means that journalists are still able to do their work and protect their sources. EU Member States shall, when necessary, provide for exemptions or derogations to the press in their national laws.

1.5.6. Myth 6: Well anyway, Facebook is based in the US...

All companies operating in the EU market will have to comply with the new rules, no matter where they are based and where their data processing activities are taking place. All companies will be subject to the same sanctions if they break the rules. This creates a level playing field for both EU and non-EU companies.

1.5.7. Myth 7: GDPR does not give us more control as companies simply ask for consent once and then they do what they want with my data

The GDPR states that personal data cannot be used without the consent of the person concerned. If a company collects a person’s data for a certain purpose, and then wants to use the data for another purpose, or forward it to a third party, they must ask for the person’s consent again. Where your consent has been requested to process your data, you can, at any point in time, ask the organisation to stop processing it by withdrawing your consent. They must do so if they have not relied on any other legal grounds for processing your data.

1.5.8. Myth 8: GDPR hinders political campaigning

The GDPR does not ban political parties and campaign groups from processing personal data for political purposes. But the rules do clarify that they are only allowed to do this for reasons of public interest and provided that appropriate safeguards are established.

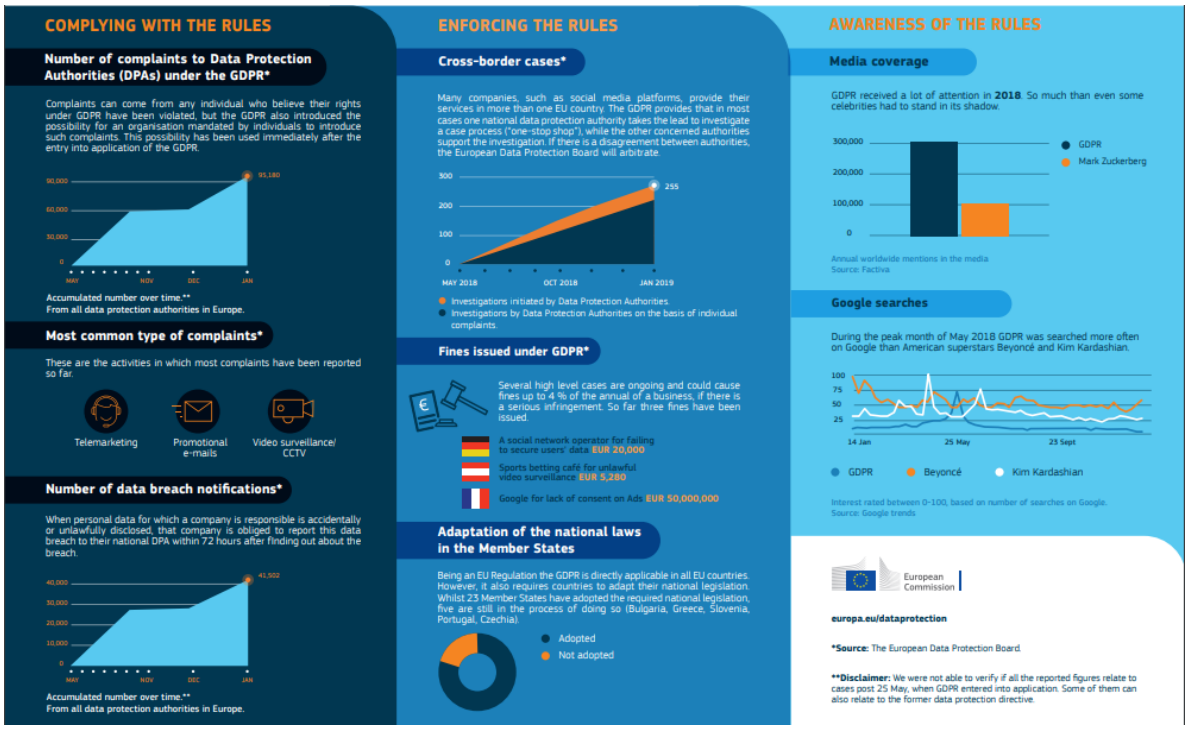
1.5.9. Myth 9: We need more time to adapt to these complicated rules

When the GDPR came into force on 24 May 2016, a two-year transition period was provided to give companies time to bring their practices into line with the new rules. This transition period ended on 25 May 2018. As of now, the data protection supervisory authorities have the power to sanction those who are not compliant with the new rules.

1.5.10. Myth 10: The fines under GDPR can kill a business

The GDPR establishes a range of penalties for those who break rules. As well as fines, there are other corrective measures like warnings, reprimands and orders to comply with data subject's requests. The data protection supervisory authorities' decision to impose fines must be proportionate and based on an assessment of all the circumstances of the individual case. If they decide to impose a fine, then €20 million or 4% of annual turnover is the absolute maximum amount. The amount of the fine depends on the circumstances in the individual case, including the gravity of the infringement or if the infringement was intentional or negligent.

Figure 2. GDPR in numbers



Source: European Commission (2019

2. WEB SAFETY INITIATIVES

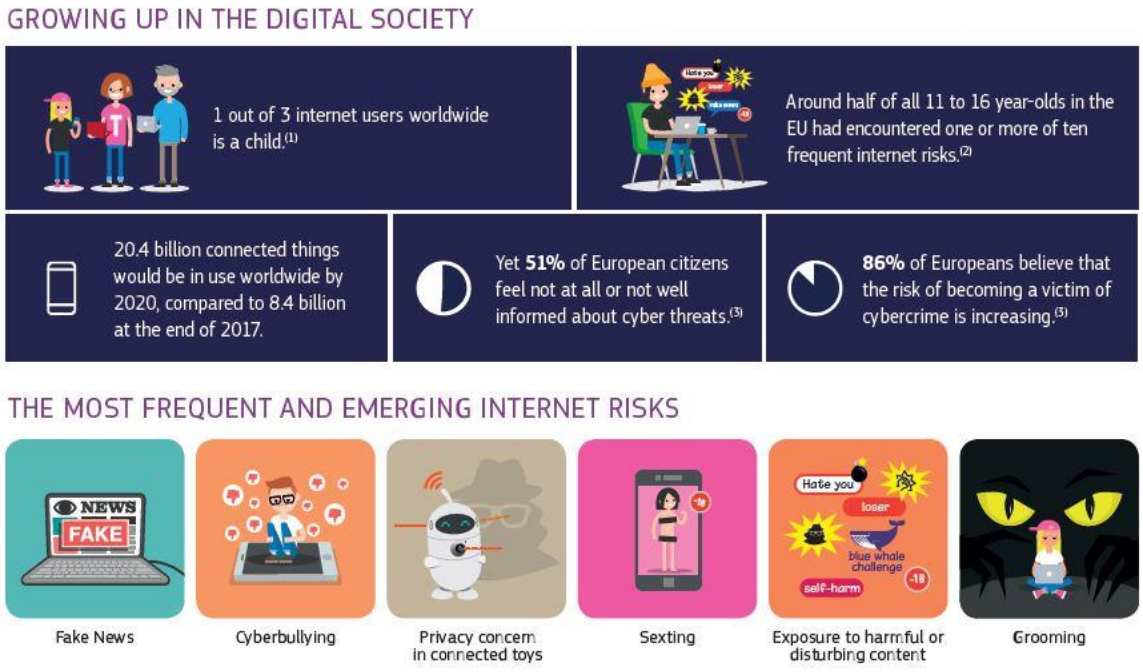
2.1. A EUROPEAN STRATEGY TO DELIVER A BETTER INTERNET FOR OUR CHILDREN

The Digital Agenda for Europe aims to have every European digital. Children have particular needs and vulnerabilities on the internet; however, the internet also provides a place of opportunities for children to access knowledge, to communicate, to develop their skills and to improve their job perspectives and employability.

The 'Strategy for a Better Internet for Children' proposes a series of actions to be undertaken by the Commission, Member States and by the whole industry value chain. Find out more on the EC website: https://www.betterinternetforkids.eu/.

In reaching this point however, EC policy has evolved over the course of a number of years and via various programmes. To help track this process, we have developed a policy roadmap aiming to provide a chronological overview of the various relevant activity lines and stakeholders involved, including programme timelines, key outreach events and campaigns, the role of industry, as well as the ongoing evaluation processes.

Figure 3. Growing up in the Digital Society



Source: European Commission (n.d.)

The European Strategy for a Better Internet for Children provides a set of complementary measures, ranging from funding, coordination and self-regulation.

The Commission co-funds Safer Internet Centres in Member States (coordinated by Insafe), with the Better Internet for Kids portal as a single entry point for resources and sharing best practices across Europe. Their main task is to raise awareness and foster digital literacy among minors, parents and teachers. They also fight against online child sexual abuse material through its network of hotlines (INHOPE).

The Commission is facilitating the "Alliance to better protect minors online", a self-regulatory initiative with leading ICT and media companies, civil society and industry associations tackling harmful online content and behaviour.

2.1.1. European framework

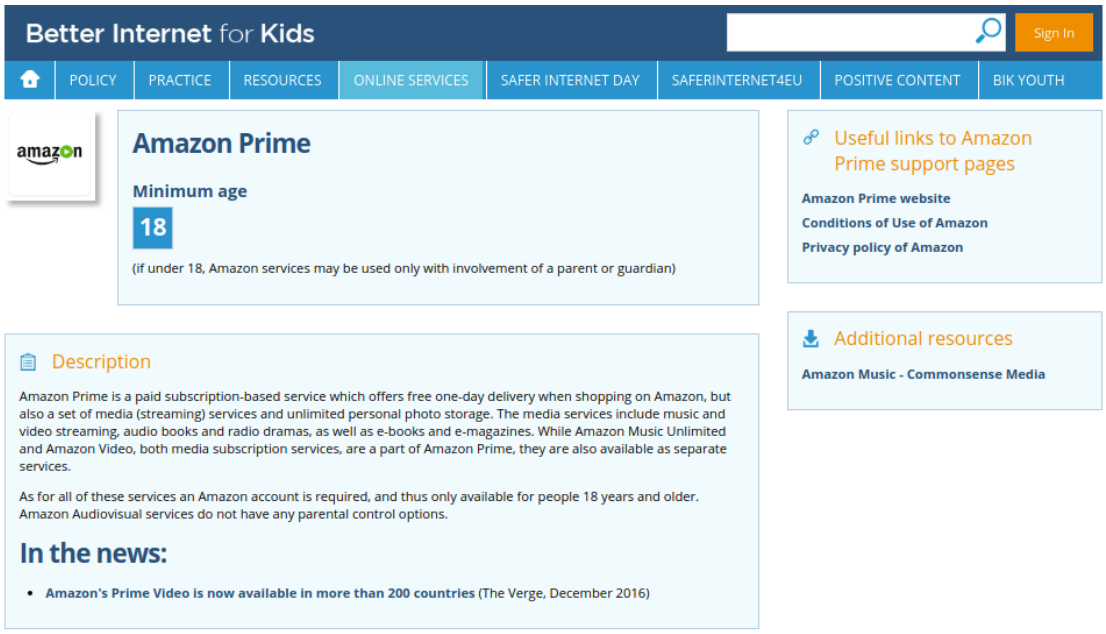
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - European Strategy for a Better Internet for Children.

2.1.2. An overview of the strategy activities

Guide to online services

The Better Internet for Kids (BIK) guide to online services aims to provide key information about some of the most popular apps, social networking sites and other platforms which are commonly being used by children and young people (and adults) today.

Figure 4. Example of guide to online services (Amazon Prime)



Source: Better Internet for Kids (n.d.)

Safer Internet Day

Safer Internet Day (SID) is an international event taking place in February every year, which promotes a safer and more responsible use of online technology and mobile phones by children and young people across the world.

Figure 5. Logo of safer internet day 2020

Source: Safer Internet Day (2019)

Over the years, Safer Internet Day (SID) has become a landmark event in the online safety calendar. Starting as an initiative of the EU SafeBorders project in 2004 and taken up by the Insafe network, Safer Internet Day has grown beyond its traditional geographic zone and is now celebrated in more than 100 countries worldwide, and across six of the world's seven continents.

From cyberbullying to social networking each year SID aims to address the current issues that influence especially young users online. Internet is a powerful tool with enormous opportunities for learning, enhancing skills and acquiring new abilities and knowledge. However, with opportunities come risks. The goal of SID is to raise awareness but also to help by concrete actions to create not only a safe place but also a better place to be when being online. In order to achieve this goal SID offers the possibility for children, young students, teachers, parents, industry, policy makers, decision takers and other stakeholders to co-create better Internet.

#SaferInternet4EU campaign

A new European campaign to be launched on Safer Internet Day 6th February 2018, to promote online safety, media literacy and cyber-hygiene, making children, parents and teachers more aware of digital opportunities and challenges.

The campaign is part of the recently adopted Digital Education Action Plan which sets out a series of initiatives to support citizens, educational institutions and education systems to better adapt for life and work in an age of rapid digital change.

The campaign federates efforts by different stakeholders at EU and national level involving key players in the digital and media landscape.

The campaign will run throughout 2018 covering a wide range of topics, including critical thinking, media literacy and digital skills necessary to identify and combat fake news and seek trusted sources of information, cyber hygiene.

Online Safety MOOC

The Online safety MOOC took place in February/March 2018. It enabled participants to gain a better understanding of new and old risks and challenges that young people face when they go online. With the course moderators, they discussed strategies for supporting young people and helping them to develop safe and responsible online and offline behaviours. A wide range of resources that can be used in schools will be provided, and participants will also be asked to share their own experiences, challenges and successes.

Key objectives were:

- To understand the importance of providing a safer and better internet for children and young people.
- To explore the opportunities that the internet provides to access knowledge, communicate and develop skills and creativity.
- To learn about online safety challenges and how to support children and young people if they encounter difficulties - including practical tips on how to handle cyberbullying, fake news, sexting and online hate speech.
- To raise awareness of, and signpost to, resources for teaching online safety in schools.
- To raise awareness of the Better Internet for Kids (BIK) strategy and Insafe network, as part of the network of Safer Internet Centres (SICs) in Europe, and associated resources.

Safer internet centers network

Safer Internet Centres raise awareness regarding online risks amongst children, parents, teachers and carers.

Safer Internet Centres are made up of awareness centres and helplines (organised in a pan-European network called Insafe) and hotlines (organised in a unique pan-European network

called International Association of Internet Hotlines - INHOPE), in all the Member States, Iceland, Norway and Russia.

Insafe and INHOPE work together through a network of Safer Internet Centres (SICs) across Europe – typically comprising an awareness centre, helpline, hotline and youth panel.

National awareness centres focus on raising awareness and understanding of safer internet issues and emerging trends. They run campaigns to empower children, young people, parents, carers and teachers with the skills, knowledge and strategies to stay safe online and take advantage of the opportunities that internet and mobile technology provides.

Helplines provide information, advice and assistance to children, youth and parents on how to deal with harmful content, harmful contact (such as grooming) and harmful conduct such as (cyberbullying or sexting). Helplines can increasingly be accessed via a variety of means - telephone, email, web forms, Skype, and online chat services.

Hotlines exist to allow members of the public to report illegal content anonymously. Reports are then passed on to the appropriate body for action (internet service provider, Law Enforcement Agency in the country or corresponding INHOPE Association Hotline).

Youth panels allow young people to express their views and exchange knowledge and experiences concerning their use of online technologies, as well as tips on how to stay safe. They also advise on internet safety and empowerment strategy, help create innovative resources and disseminate eSafety messages to their peers.

Safer Internet Forum

Safer Internet Forum is the key annual international conference in Europe under Better Internet for Kids including direct participation from young people.
Latest trends, risks and solutions related to child online safety are discussed by policy makers, researchers, law enforcement bodies, youth, parents and carers, teachers, NGOs, industry representatives, experts.

Alliance to better protect minors online

The Alliance is a self-regulatory initiative. It aims to better protect minors online by improving the online environment for children and young people.

Following the European Commission's invitation to come together and take part in a joint effort, leading ICT and media companies, NGOs and Unicef officially launched the Alliance on Safer Internet Day 2017.

This multi-stakeholder platform is open to new members and builds on the previous work of the CEO Coalition. The companies will address emerging risks that minors face online, such as harmful content (e.g. violent or sexually exploitative content), harmful conduct (e.g. cyberbullying) and harmful contact (e.g. sexual extortion).

The Statement of Purpose of the Alliance introduces nine actions under three main strands:

1. Identifying and promoting best practice for the communication of data privacy practices;
2. Providing accessible and robust tools that are easy to use and to provide feedback and notification as appropriate;
3. Promoting users' awareness and use of information and tools to help keep themselves safer online and of their responsibility and duty to behave responsibly and respectfully towards others and foster trust, at the same time promoting minor's digital empowerment;
4. Promoting use of content classification when and where appropriate;
5. Promoting the awareness and use of parental control tools.
6. Intensifying cooperation with other parties such as Child Safety Organisations Governments, education services and law enforcement to enhance best practice-sharing;
7. Identifying emerging developments in technology such as connected devices and, with the support of the Commission, engage with other parties who also have a role to play in supporting child safety online.
8. Supporting the development of awareness-raising campaigns about online safety, digital empowerment, and media literacy through both ad hoc and ongoing initiatives;
9. Promoting children's access to diversified online content, opinions, information and knowledge.

Table 1. Alliance members

- **Company signatories:** ASKfm, BT Group, Deutsche Telekom, Disney, Facebook, Google, KPN, The LEGO Group, Liberty Global, Microsoft, Orange, Rovio, Samsung Electronics, Sky, Snap, Spotify, Sulake, Super RTL/Mediengruppe RTL Deutschland, TIM (Telecom Italia), Telefónica, Telenor, Telia Company, Twitter, Vivendi, Vodafone.
- **Associated:** BBFC, Child Helpline International, COFACE, eNACSO, EUN Partnership, FFTelecoms, FOSI, FSM, GSMA, ICT Coalition, NICAM, Toy Industries of Europe, UNICEF.

2.2. THE EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA)

The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. The Agency is located in Greece with its seat in Athens and a branch office in Heraklion, Crete.

ENISA is actively contributing to a high level of network and information security (NIS) within the Union, since it was set up in 2004, to the development of a culture of NIS in society and in order to raise awareness of NIS, thus contributing to proper functioning of the internal market.

The Agency works closely together with Members States and private sector to deliver advice and solutions. This includes, the pan-European Cyber Security Exercises, the development of National Cyber Security Strategies, CSIRTs cooperation and capacity building, but also studies on secure Cloud adoption, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, and identifying the cyber threat landscape, and others. ENISA also supports the development and implementation of the European Union's policy and law on matters relating to NIS.

ENISA's approach is illustrated below by presenting its activities in three areas:

- Recommendations.
- Activities that support policy making and implementation.
- 'Hands On' work, where ENISA collaborates directly with operational teams throughout the EU.

2.2.2. European framework

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.

Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

2.2.3. An overview of the ENISA activities

Annual Privacy Forum

The APF seeks to contribute to the implementation of information security in the area of privacy and personal data protection. The APF is set against the EU legislative background that mainly, but not exclusively, comprises the General Data Protection Regulation (GDPR) and the draft ePrivacy Regulation (ePR). The APF sets the stage for discussions of research proposals, solutions, models, applications and policies. In the last few years, the APF has also developed a deeper industry footprint, to complement its original research and policy orientation.

For more information, please visit: https://privacyforum.eu/

Cyber threat report

The ENISA Threat Landscape provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends. Hundreds of reports from security industry, networks of excellence, standardisation bodies and other independent institutes have been analysed.

ETL 2018

The ENISA Threat Landscape 2018 provides a comprehen-sive compilation of top 15 cyberthreats encoutnered within the time period December 2017 - December 2018. 2018 was a year that has brought significant changes in the cyberthreat landscape. Those changes had as source discrete developments in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors. Monetization motives have contributed to the appearance of crypto-miners in the top 15 threats. State-sponsored activities have led to the assumption that there is a shift towards reducing the use of complex malicious software and infrastructures and going towards low profile social engineering attacks. These developments are the subject of this threat landscape report.

European Cyber Security Month

European Cyber Security Month (ECSM) is an EU awareness campaign that promotes cyber security among citizens and organizations about the importance of information security and highlighting the simple steps that can be taken to protect their data, whether personal, financial and/or professional. The main goal being to raise awareness, change behaviour and provide resources to all about how to protect themselves online. The European Union Agency for Network and Information Security (ENISA), the European Commission DG CONNECT and Partners are deploying the European Cyber Security Month (ECSM) every October.

The objectives of the European Cyber Security Month:

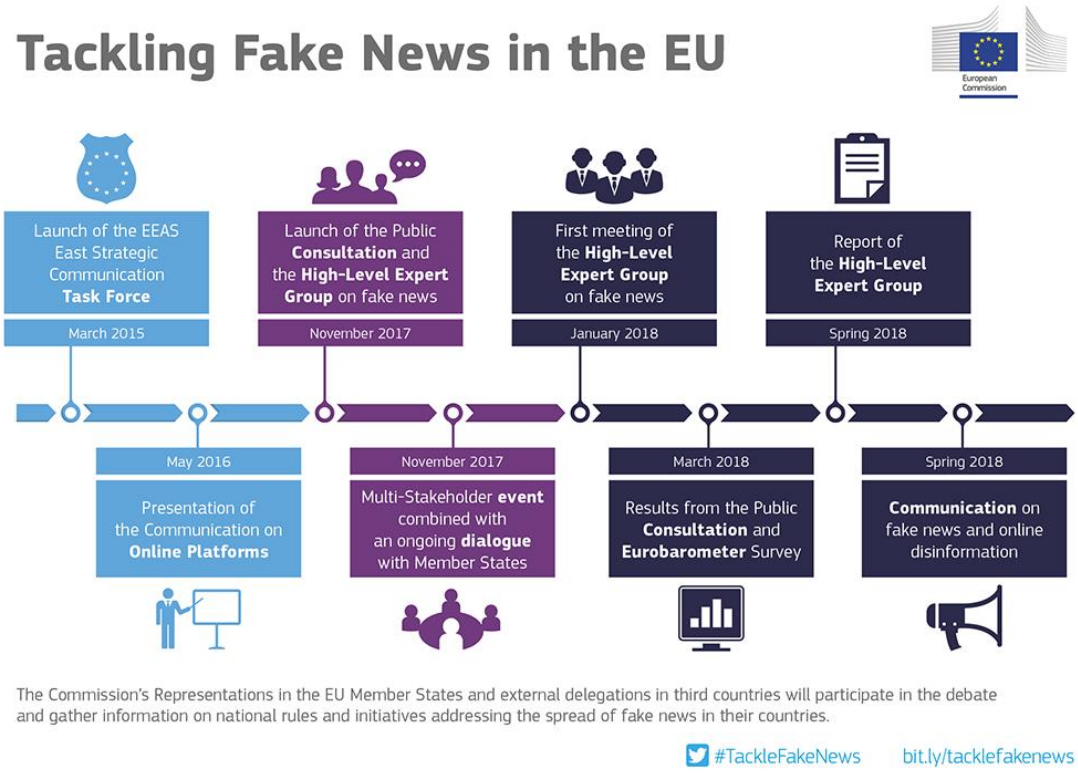
- generate general awareness about cyber security, which is one of the priorities identified in the EU Cyber Security Strategy;
- generate specific awareness on Network and Information Security (NIS), which is addressed in the proposed NIS Directive;
- promote safer use of the Internet for all users;
- build a strong track record to raise awareness through the ECSM;
- involve relevant stakeholders;
- increase national media interest through the European and global dimension of the project;
- enhance attention and interest with regard to information security through political and media coordination.

Learning materials: https://cybersecuritymonth.eu/get-cyber-skilled/education-modules

3. FAKE NEWS

The exposure of citizens to large scale disinformation, including misleading or outright false information, is a major challenge for Europe. The Commission has engaged with all stakeholders to define a clear, comprehensive and broad-based action plan to tackle the spread and impact of online disinformation in Europe and ensure the protection of European values and democratic systems.

Figure 6. Tackling Fake News in the EU



Source: European Commission (2018)

Disinformation - or fake news - consists of verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm.

The phenomenon is having a bigger impact than ever before as it is easier for anyone to post and share any news or information online.

Social media and online platforms play an important role in speeding up the spread of such news and they enable a global reach without much effort from the author.

A comprehensive policy response must reflect the specific roles of different actors (social platforms, news media and users), and define their responsibilities according to a number of guiding principles. These include the freedom of expression, media pluralism, and the rights of citizens to diverse and reliable information.

The Commission supports a multi-stakeholders process, involving platforms, news media, research and civil society organisations in order to find the right solutions consistent with fundamental principles and applicable coherently across the European Union.

The European Union has outlined an action plan to step up efforts to counter disinformation in Europe and beyond focusing on four key areas. This plan serves to build EU's capabilities and strengthen cooperation between member states by improving detection, having a coordinated response to threats, collaboration with online platforms and industry as well as raising awareness and empowering citizens. The factsheet on the action plan to counter disinformation provides a clear overview.

A first Report assessing the progress made in the implementation of the actions set out in the April Communication on online disinformation was also adopted.

The Action Plan complements the Communication "Tackling online disinformation: a European approach", that puts forward self-regulatory tools to tackle the spread and impact of online disinformation in Europe, and ensure the protection of European values and democratic systems.

Four principles guide the action:

1. Improve transparency regarding the way information is produced or sponsored;
2. Diversity of information;
3. Credibility of information;
4. Inclusive solutions with broad stakeholder involvement.

The Communication on online disinformation has been developed taking into account the extensive consultations with citizens and stakeholders:

- a public consultation to gather the views of a wide range of stakeholders on fake news. The synopsis report is now available. The consultation process was complemented with a Eurobarometer public opinion survey to measure and analyse the perceptions and concerns of the European citizens around fake news.
- a multi-stakeholder conference and a colloquium on fake news to define the boundaries of the problem, assess the effectiveness of the solutions already put in place by social media platforms and to agree on key principles for further action.
- a High Level Group (HLG), to advise on policy initiatives to counter fake news and the spread of disinformation online. The Group submitted its final report on the 12 March 2018. You can check the list of members.
- a self-regulatory Code of Practice to address the spread of online disinformation and fake news is now in place as a step forward to ensure transparency and fairness in online campaigns.
- individual roadmaps by online platforms and the advertising industry to implement the Code of Practice.

As European Commission President Juncker mentioned in his mission letter to Commissioner for the Digital Economy and Society Mariya Gabriel, the Commission needs to look into the challenges the online platforms create for our democracies as regards the spreading of fake information and initiate a reflection on what would be needed at EU level to protect our citizens.

In April 2017, Vice-President Andrus Ansip in charge of the completion of the Digital Single Market described fake news as a serious problem. At the same time he highlighted the need to protect freedom of speech and trust people's common sense. He also mentioned media literacy and quality journalism as vital tools to address the spread of fake news online.

3.1. EUROPEAN FRAMEWORK

Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Action Plan Against Desinformation.

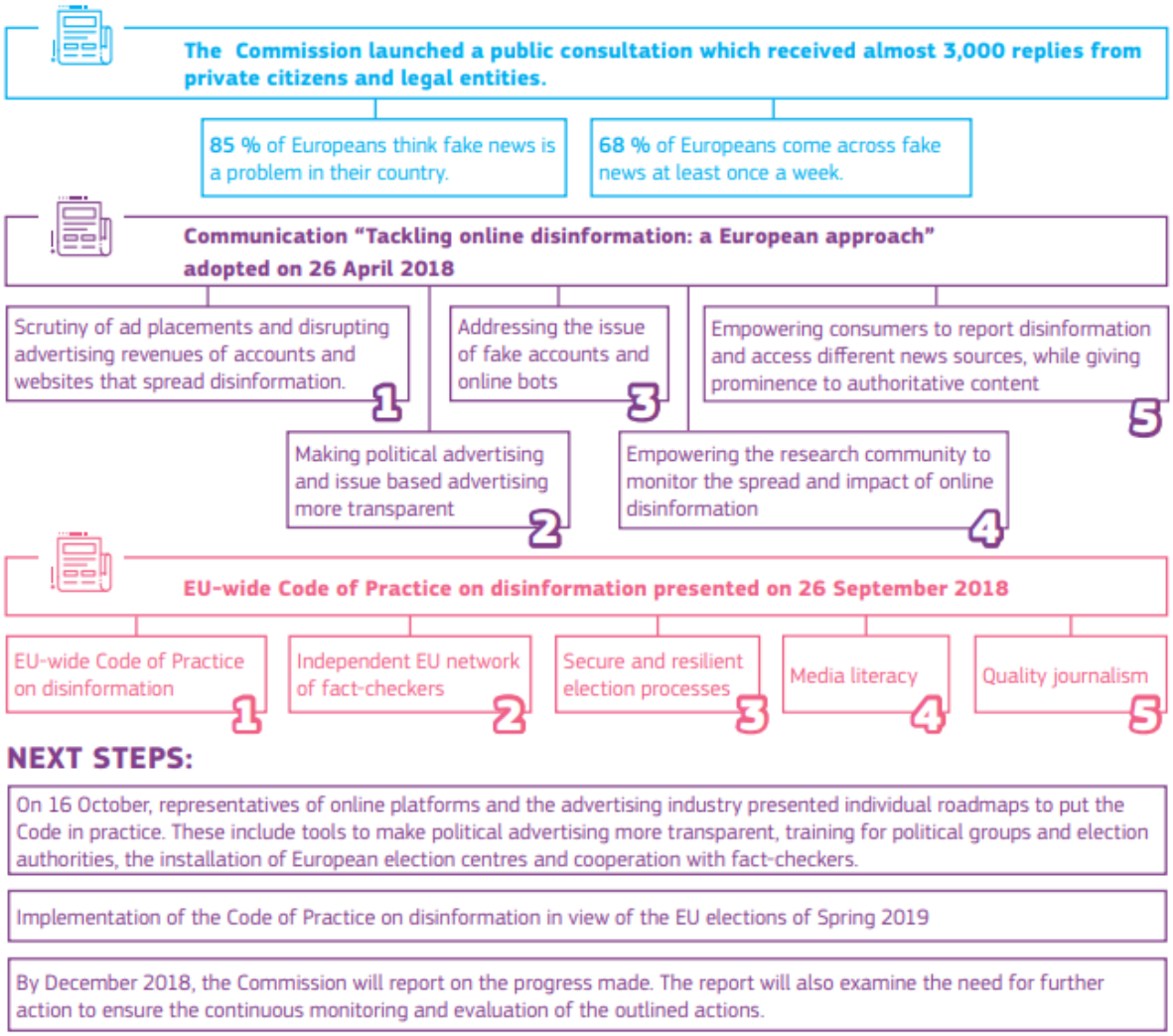
3.2. THE EU STEPS UP ACTION AGAINST DISINFORMATION

What has the EU done so far to counter disinformation?

Disinformation– i.e. verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public - distorts public debate, undermines citizens' trust in institutions and media, and even destabilises democratic processes such as elections. 73% of internet users in the EU are concerned about disinformation in pre-election periods. Given its cross-border dimension, the adverse effects of disinformation in the European Union require a coordinated and long-term approach to respond to the challenge at both EU and national level.

In 2015, after the European Council's call to address the ongoing disinformation campaigns by Russia, the East Stratcom Task Force was created in the European External Action Service (EEAS). To date, the Task Force has catalogued, analysed and raised awareness of over 4,500 examples of pro-Kremlin disinformation, and significantly improved understanding of the tools, techniques and intentions of disinformation by Russian sources. In close cooperation with European Commission services, it has also substantially improved the effectiveness of EU communications in the Eastern Neighbourhood.

Figure 7. Steps taken to counter desinformation



Source: European Commision (2018)

In 2016, the Joint Framework on countering hybrid threats was adopted, followed by the Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats in 2018. As part of the measures foreseen in this context, the Hybrid Fusion Cell was created in the EEAS in 2016 to act as a single focus for the analysis of hybrid threats for EU institutions, and in 2017 the European Centre of Excellence for Countering Hybrid Threats was established in Helsinki.

The Commission put forward a European approach for tackling online disinformation in its Communication of April 2018, seeking to promote a more transparent, trustworthy and accountable online environment. The Communication proposed measures to tackle disinformation online, including a self-regulatory EU-wide Code of Practice on Disinformation, signed by large online platforms and the advertising industry, as well as support for an independent network of fact-checkers. The Communication also stressed the need to ensure secure and resilient election processes, to foster education and media literacy, and to support quality journalism. The Commission also called for a strengthening of strategic communications.

On 12 September 2018, the Commission set out measures to secure free and fair European elections, including greater transparency in online political advertisements and the possibility to impose sanctions for the illegal use of personal data in order to deliberately influence the outcome of the European elections.

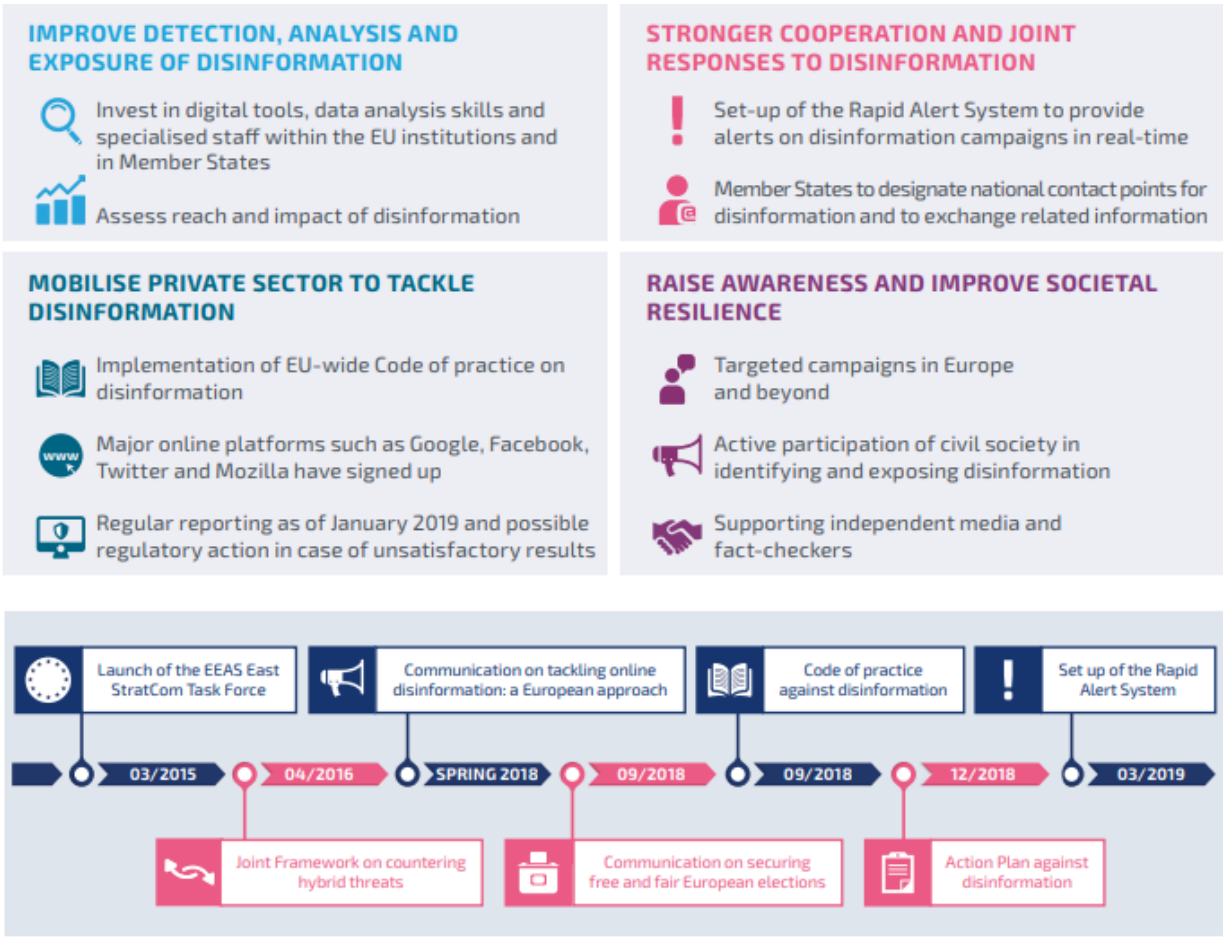
Building on these efforts, the EU has today presented an Action Plan with additional measures to counter disinformation and is reporting on the progress so far in tackling online disinformation.

3.2.1. Action Plan against Disinformation

What does this Action Plan propose and why? How does it complement existing initiatives?

The Action Plan proposes a set of actions that should further enable a joint and coordinated EU approach to addressing disinformation.

Figure 8. Action Plan against Desinformation



Source: European Commission (2018)

To step up the EU's response to disinformation, the Action Plan focuses on four pillars:

- Improving the capabilities of the Union's institutions to detect, analyse and expose disinformation;
- Strengthening coordinated and joint responses by EU institutions and Member States to disinformation;
- Mobilising the private sector to tackle disinformation; and
- Raising awareness about disinformation, and improving societal resilience.

The European Commission and the High Representative will develop and implement these actions, in close cooperation with Member States and the European Parliament.

With six months left before the European elections, how timely is the Action Plan?

Very timely. The Action Plan sets out a number of concrete actions and all actors are expected to coordinate and work together as a matter of priority to maximise the EU's preparedness ahead of the European elections in May 2019. In that sense, it complements the actions the Commission announced in the September 2018 with its Communication on Securing free and fair European elections and the April 2018 Communication on Tackling online disinformation. The EU institutions have already built an internal network against disinformation and are in parallel working on strengthening their strategic communication capacities.

What resources does the Commission plan to allocate for the implementation of these actions?

The EEAS' strategic communication budget to address disinformation and raise awareness about its adverse impact is expected to more than double, from €1.9 million in 2018 to €5 million in 2019. This will also be accompanied by a reinforcement of staff (an increase of 50-55 staff member is planned over the next two years).

This represents an important step, as the East Stratcom Task Force of the EEAS, while created in 2015, received dedicated resources only in 2018 when a budget of €1.1 million was allocated under the 2018 Preparatory Action: 'StratCom Plus', proposed by the European Parliament. In addition, €800,000 were allocated to the EEAS for strategic communication.

This first dedicated budget for the disinformation work allows for a more professional and technical monitoring of the information space in the Eastern Partnership countries and of Russian media (operating in Russia and beyond). Combining a qualitative approach with a quantitative one in detecting emerging trends in relation to the EU and its policies, the Action provides: wider geographic and language coverage of media monitoring; systematic data monitoring and analysis; and inputs from experts on disinformation in the Eastern Partnership region.

In addition, in its proposal for Horizon Europe programme (2021-2027), the Commission has foreseen funding for the development of new tools to combat online disinformation; to better understand the role of journalistic standards and user-generated content; and to support next generation internet applications and services including immersive and trustworthy media, social media and social networking. So far around €40 million have been invested in EU projects in the area.

The Commission also proposed a dedicated budget of €61 million under the next Creative Europe programme to support journalism, media freedom, media pluralism and media literacy.

What role does the Action Plan envisage for the EU Member States?

The Action Plan sets out key actions to tackle disinformation in a coordinated approach among the EU institutions and in cooperation with the Member States. The Plan calls for the strengthening of cooperation in detecting, analysing and exposing disinformation campaigns, and in raising awareness about the negative impact of disinformation. Among others, it includes proposals that Member States designate national contact points that would participate in the Rapid Alert System. The Rapid Alert System would facilitate common situational awareness and a coordinated response. Complementary to EU institutions' efforts, Member States should raise awareness of the negative impact of disinformation and support the work of independent media, fact-checkers and investigative journalists, including through the creation of multidisciplinary teams with specific knowledge about local information environments.

What is the Rapid Alert System and how will it work?

When democracy in one Member State is under attack, European democracy as a whole is under attack. A strong European response requires Member States and EU institutions to work together much more closely, and to help each other understand and confront the threat. The Rapid Alert System will build on a secure digital platform, where Member States can share information on ongoing foreign disinformation campaigns with one another, and coordinate responses. The Rapid Alert System will be based on open-source and unclassified information only, and will exclusively focus on coordinated attempts by foreign actors to manipulate free and open debate. In view of setting up the Rapid Alert System by March 2019, each Member State should designate a contact point, ideally positioned within strategic communication departments.

Does the EU plan to coordinate its actions with international actors or fora, for example NATO or G7?

Cooperation on threat analysis and situational awareness with NATO is ongoing. G7 partners are in the process of establishing a Rapid Response Mechanism to reinforce the defences of democracies. The Commission and the High Representative will continue regular exchanges of information with key partners in the framework of ongoing staff-to-staff cooperation. This will also be used to promote information exchange and best practices.

What will the Commission do to improve the media literacy of online users?

As part of the Media Literacy Week in March 2019, in cooperation with the Member States, the Commission will support cross-border cooperation amongst media literacy practitioners as well as the launch of practical tools for the promotion of media literacy to the public. The Action Plan also calls upon Member States to ensure a rapid and effective implementation of the provisions of the Audio-visual Media Services Directive concerning media literacy.

What are the Action plan and the EU doing to support the media?

The Commission supports quality news media and journalism as an essential element of a democratic society. As confirmed in the progress report, the Commission wants to enhance transparency and predictability of State aid rules for the media sector; it also launched a call of about €1.9 million for production and dissemination of quality news content, which is still ongoing. To favour quality journalism, media freedom, media literacy and media pluralism, the Commission proposed a dedicated budget in the 2021-2027 Creative Europe, addressing the structural changes faced by the media sector. Finally, the Commission co-funds, together with initiatives of the European Parliament, independent projects in the field of media freedom and pluralism. These projects, among other actions, monitor risks to media pluralism across Europe, map violations to media freedom, fund cross-border investigative journalism and support journalists under threat.

What is the role of the European network of fact-checkers in tackling online disinformation?

Fact-checkers are essential in tackling disinformation. They verify and assess the veracity of content based on facts and evidence thus helping the information ecosystem to be cleaner and more robust. The Commission aims to foster the cooperation between European fact-checkers and therefore supports the creation of a network of European fact-checkers. The fact-checking community will define the prerequisites for membership in the coming months. The network will be editorially independent. Regarding the online platform to connect fact-checkers and researchers, an initial funding of €2.5 million under the Connected Europe Facility instrument (CEF) is foreseen.

As a first step, the Commission will offer online tools to fact-checkers to enable their collaboration. As a second step, the Commission will deploy a secure European online platform on disinformation. This will offer cross-border data collection, analysis tools and access to EU-wide data, in support of cooperation between the fact-checking community and academics working on the problem of online disinformation.

3.2.2. Code of Practice

What is the role foreseen for the industry, e.g. social media platforms, advertisers or the advertising industry?

Industry has a very important role to play in effectively tackling this problem, mainly due to the use of new technologies and social media to spread, target and amplify disinformation. In October, main online companies (Google, Facebook, Twitter and Mozilla) signed a Code of Practice committing themselves to a number of actions ahead of European elections. The Action Plan underlines that they should immediately ensure the transparency of political advertising, take decisive action against fake accounts and identify automated bots and label them accordingly. The Action Plan also urges the platforms to cooperate with national contact points on disinformation and with fact checkers to help effectively fight disinformation. Their full commitment to the Code of Practice and the swift and effective implementation of key measures is important for granting safe and fair elections and secure a more transparent online environment.

How will the Commission monitor the implementation of the Code of Practice signed by online platforms and adverting sector?

The Commission will ask the signatories for up-to-date information about measures taken towards the implementation of the Code by the end of 2018 and will publish this information in January 2019. Moreover, beginning in January, platforms should provide complete information, including by replying to Commission's specific requests, on how are they are implementing the commitments on a monthly basis. In the autumn, the Commission will carry out a targeted monitoring of the implementation of the Code on a monthly basis. The Commission will seek the assistance of the European Regulators Group for Audio-visual Media Services, the independent network of audio-visual regulators under the Audio-visual Media Services Directive, in monitoring the implementation of the Code in the various Member States.

Why does the Commission think that self-regulation for online platforms is the right approach to tackle the issue?

Online disinformation is a new, multi-faceted and fast developing issue that requires immediate action. Therefore, self-regulation, if correctly implemented, is an appropriate way for online platforms to take swift action to tackle this problem. By comparison, a regulatory approach would take longer to prepare and implement. Should the self-regulatory approach fail, the Commission may propose further actions, including regulatory ones.

What are platforms doing to avoid disinformation in the run up to the EU elections?

The online platforms which have signed the Code of Practice have provided individual roadmaps detailing the key tools and policies they will apply in all EU Member States ahead of the

elections. These include, for example, transparency tools for political advertising, so that online political advertising distributed through social media is clearly marked as such and is distinguishable from other types of sponsored content.

The roadmaps detail each company's policies to implement the Code of Practice, structured around five themes: advertising policies; political advertising; service integrity; empowering consumers and empowering the research community.

Does the Commission trust the platforms to implement the Code?

Subscription to the Code is voluntary. However, there are growing expectations that online platforms should not only comply with legal obligations under EU and national laws, but also act with appropriate responsibility to protect users from disinformation.

The Commission expects the signatories to implement the Code on a full, effective and timely basis. To this end, the Commission will closely monitor implementation and assess the effectiveness of the Code. The platforms should by the end of this year provide the Commission with up-to-date and complete information on the actions they have taken to comply with their commitments. The Commission will publish this information in January 2019. The Commission will then make a first assessment of the implementation of the Code at the end of the year.

3.3. STUDY ON FAKE NEWS AND DISINFORMATION FROM THE EUROPEAN COMMISSION'S JOINT RESEARCH CENTRE

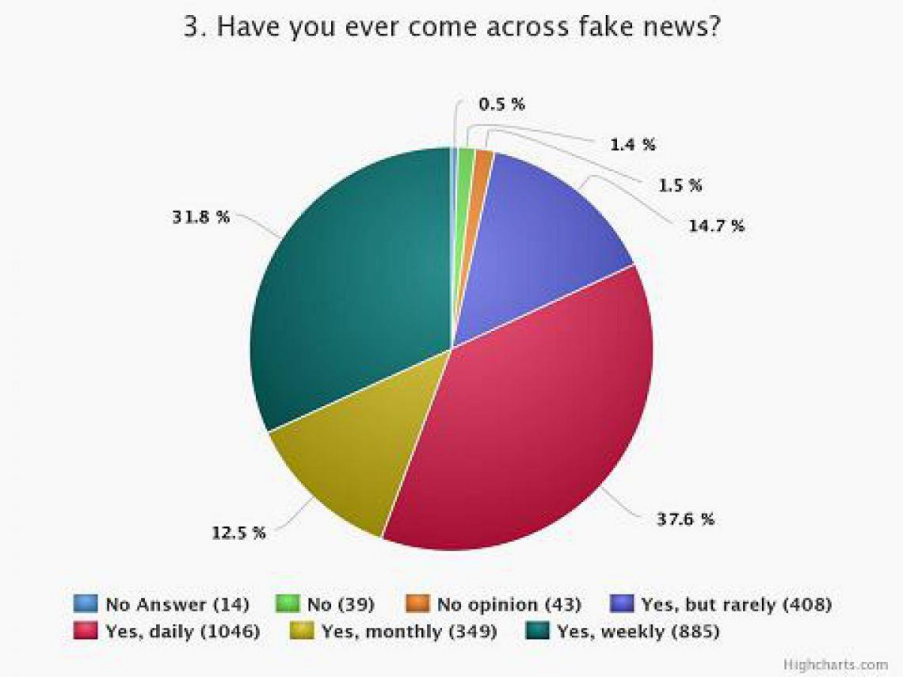
This report contains an overview of the relevant economic research literature on the digital transformation of news markets and the impact on the quality of news. It compares various definitions of fake news, including false news and other types of disinformation and finds that there is no consensus on this. It presents some survey data on consumer trust and quality perceptions of various sources of online news that indicate relatively high trust in legacy printed and broadcasted news publishers and lower trust in algorithm-driven news distribution channels such as aggregators and social media. Still, two thirds of consumers access news via these channels. More analytical empirical evidence on the online consumption of genuine and fake news shows that strong newspaper brands continue to attract large audiences from across the political spectrum for direct access to newspaper websites. Real news consumption on these sites dwarfs fake news consumption. Fake news travels faster and further on social media sites. Algorithm-driven news distribution platforms have reduced market entry costs and widened the market reach for news publishers and readers. At the same time, they separate the role of content editors and curators of news distribution. The latter becomes algorithm-driven, often with a view to maximize traffic and advertising revenue. That weakens the role of trusted editors as quality intermediaries and facilitates the distribution of false and fake news content. It might lead to news market failures.

News distribution platforms have recently become aware of the need to correct for these potential failures. Non-regulatory initiatives such as fact-checking, enhanced media literacy and news media codes of conduct can also contribute.

3.4. REPORT ON PUBLIC CONSULTATION ON FAKE NEWS AND ONLINE DISINFORMATION

The public consultation took place between 13 November 2017 and 23 February 2018. The aim of the consultation was to help assess the effectiveness of current actions by market players and other stakeholders, the need for scaling them up and introducing new actions to address different types of fake news.

Figure 9. Have your ever come across fake news?



Source: European Commision (2018)

Objective of the consultation

The results of the public consultation will help assess the effectiveness of current actions by market players and other stakeholders, the need for scaling them up and introducing new actions to address different types of fake news.

The consultation will collect information on:

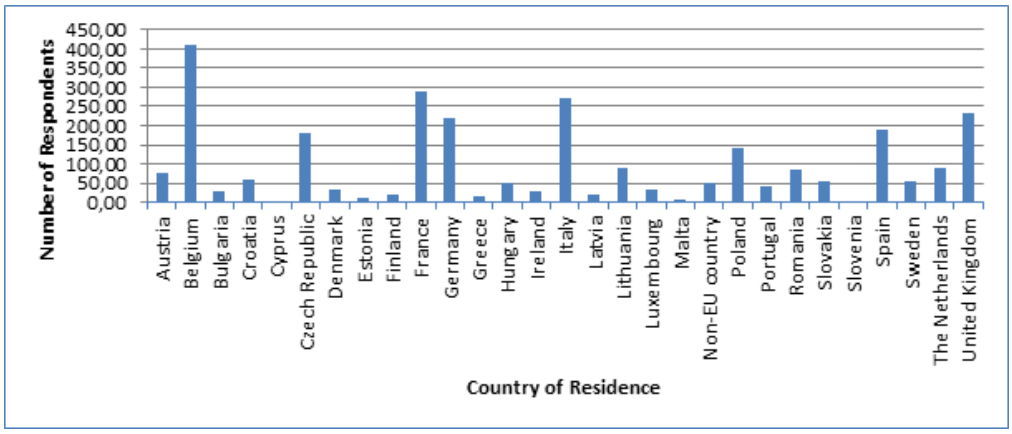
1. Definition of fake information and their spread online
2. Assessment of measures already taken by platforms, news media companies and civil society organisations to counter the spread of fake information online
3. Scope for future actions to strengthen quality information and prevent the spread of disinformation online.

Who replied to the consultation?

Two questionnaires were available: one for the citizens and one for legal persons and journalists reflecting their professional experience of fake news and online disinformation.

The public consultation received 2986 replies: 2784 from individuals and 202 from legal organisations and journalists. The largest number of replies came from Belgium, France, the United Kingdom, Italy and Spain. It is worth noting a high participation in Lithuania, Slovakia and Romania.

As regards replies from legal entities, the largest proportion of respondents represented private news media companies, followed by civil society organisations, other type of organisations, online platforms, research and academia and public authorities (national and local). Many respondents are active all around the world or in a large number of EU countries, including Belgium, France, Italy, Spain, Germany and the UK. Sixty-nine news media organisations, fifty-one civil society organisations and sixteen online platforms replied.



Source: European Commision (2018)

Key findings

There is a common perception amongst all respondents that fake news in general are highly likely to cause harm to society, in particular in areas such as political affairs, immigration, minorities and security.

Fact-checking through independent news organisations and civil society organisations is considered the method that better contributes to counter the spread of disinformation online. However, a majority of citizens believe that social media platforms are not doing enough to help users to fact-check information before it is shared online.

With regard to possible future actions, a majority agreed that more should be done to reduce the spread of disinformation online. Regardless of the type of action proposed, all respondents unanimously agreed on the need to respect and guarantee overarching fundamental rights such as freedom of expression and to ensure that any approach used to tackle fake news should not promote any kind of direct or indirect censorship.

The consultation also showed a clear preference for a multi-stakeholder, multi-dimensional, self-regulatory approach, although some respondents complained about the lack of a level playing field between content producers and online social platforms and suggested some regulatory changes. Indeed, a large number of proposed principles and actions to tackle fake news focus on the role of online social platforms.

There was wide support to fact-checking as one of the ways to combat fake news, although the consultation also helped to understand that its efficiency is limited and that it should be accompanied by other measures. The consultation also provides some interesting information on possible tools to empower journalists and end-users, including the use of new technologies such as artificial intelligence and block chain. As in the case of fact-checking, it appears that the efficiency of each tool largely depends on who uses it and for which purposes.

Strengthening efforts in increasing media literacy at all levels, from school pupils to adult audience, and among actors, from end-users to journalists, and ensuring support and access by the public to trusted journalism, given its critical role in sustaining a plural, strong public opinion, were also put forward as necessary actions.

3.5. FINAL RESULTS OF THE EUROBAROMETER ON FAKE NEWS AND ONLINE DISINFORMATION

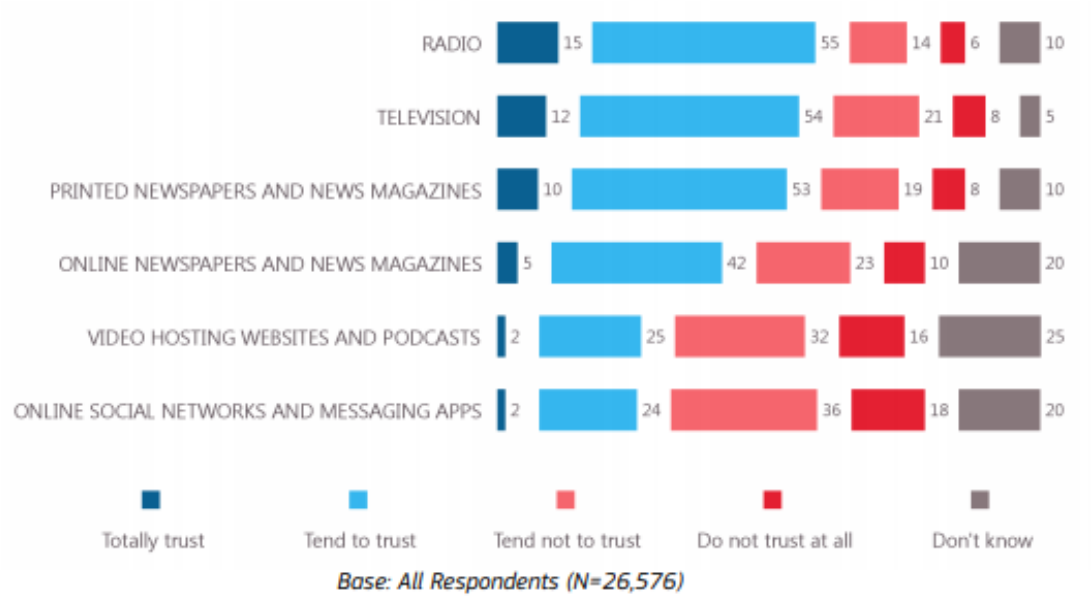
The Eurobarometer survey was conducted via telephone interviews early February in all EU Member States. Over 26.000 citizens were interviewed about their perception of fake news and their trust in news media sources. The findings show a clear concern for the spread of disinformation online in Europe.

The Flash Eurobarometer on Fake News and Online Disinformation measured the perceptions and concerns of 26.576 European citizens around fake news. The results show that fake news are widely spread across the EU with 83% of respondents saying that fake news represent a danger to democracy.

The key findings are as follows:

- Respondents perceive traditional media as the most trusted source of news: radio (70%), television (66%) and printed newspapers and news magazines (63%);

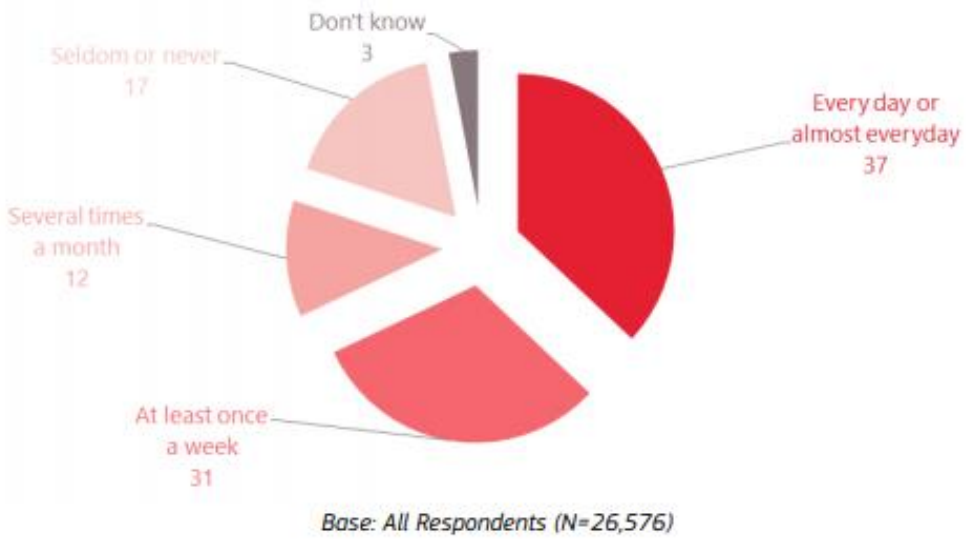
Figure 10. How much do you trust or not the news and information you access through...



Source: Flash Eurobarometer 464 (2018)

- 37% of the respondents come across fake news every day or almost everyday and 71% feel confident on identifying them;

Figure 11. How often do you come across news or information that you believe misrepresent reality or is even fake?



Source: Flash Eurobarometer 464 (2018)

- 85% of respondents perceive fake news as a problem in their country and 83% perceive it as a problem for democracy in general;
- In respondents' view, journalists (45%), national authorities (39%) and the press and broadcasting management (36%) should be the main responsible for stopping the spread of fake news.

REFERENCES

Betterinternetforkids.eu. (n.d.). *Better Internet for Kids - Home*. [online] Available at: https://www.betterinternetforkids.eu/web/portal/home [Accessed 5 Apr. 2019].

Data Protection Officer (DPO). (2019). *Legal Framework of Personal Data Protection*. [online] Available at: https://www.eca.europa.eu/sites/dpo/Pages/legalframework.aspx [Accessed 1 Apr. 2019].

Enisa.europa.eu. (2019). *ENISA*. [online] Available at: https://www.enisa.europa.eu/ [Accessed 15 Apr. 2019].

European Commission. (2019). *2018 reform of EU data protection rules*. [online] Available at: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/ 2018-reform-eu-data-protection-rules_en [Accessed 9 Apr. 2019].

European Commission. (n.d.). *Creating a Better Internet for Kids - Digital Single Market - European Commission*. [online] Available at: https://ec.europa.eu/digital-single-market/en/content/ creating-better-internet-kids-0 [Accessed 30 Mar. 2019].

European Commission. (2018). Fake news and online disinformation. [online]. Available at: https://ec.europa.eu/digital-single-market/en/fake-news-disinformation [Accessed 12 Mar. 2019]

Flash Eurobarometer 464 (2018). Fake news and desinformation report [online]. Available at: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/ getsurveydetail/instruments/flash/surveyky/2183 [Accessed 3 Apr. 2019].

Saferinternetday.org. (2019). *Safer Internet Day - Home*. [online] Available at: https://www.saferinternetday.org/web/sid/home [Accessed 3 Apr. 2019].