

# Course Support for the Development of Social Media Literacy in schools

What is the GDPR?

What is personal data?

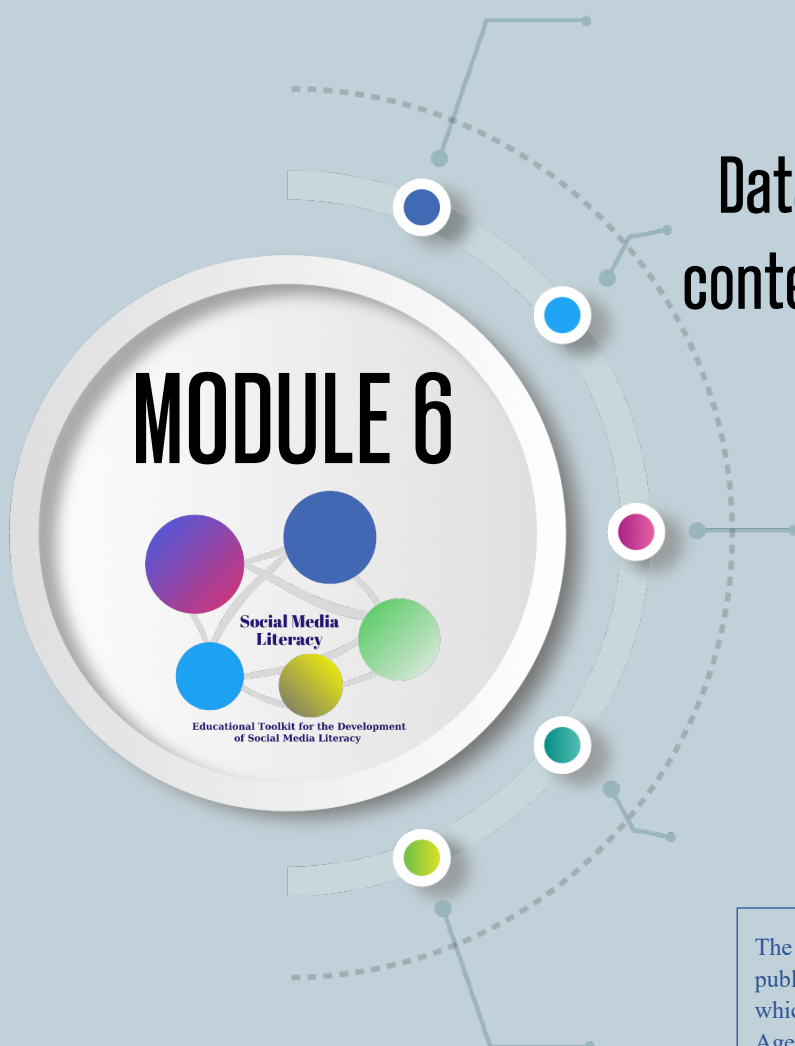
What is processing?

Who has to follow the GDPR rules?

The rules of GDPR

Targeted/behavioural advertising

What to do in case of infringements



## Data protection rules in the context of social media – GDPR

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



Erasmus+ ref.no. 2019-1-R001-KA201-063996

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the National Agency and Commission cannot be held responsible for any use which may be made of the information contained therein.

## Module aim

---

When turning to social media, privacy and data protection inevitably come into play.

Today's digital world allows us to share everything with everyone. All types of people, organisations, companies and even the government process information about you, think of your school, your commune or city, your sports club, your employer etc. However, most information about you is collected through the internet. Especially on social networking sites, such as Facebook and Instagram, a lot of personal information is being shared. A common misconception is that the services of social media platforms are free of charge: in reality you do pay, but instead of with money, you pay with your personal data. While this can be a nice way to engage with friends and even a fun means to make new friends, sharing personal information also has risks to it. Everything you share online can leave digital footprints. Once a photo, video, status, tweet etc. is posted on the internet (e.g. on your social media profile), you no longer have control over it: anyone can copy, repost or save the photo, making it impossible to completely erase it from the internet. These digital footprints can be 'personal data' (e.g. your name, your (e-mail) address, your date of birth, your pictures). Sharing this type of data can expose you to all kinds of risks (e.g. identity theft, harassment, personalized content, targeted advertising and much more). Therefore, it is important to know what personal data about you is being collected, in what manner, for how long and what is being done to protect your personal data. This is where the legislator has stepped in.

Your personal data cannot simply be used by others, nor can you use other people's personal data. For quite some time already, there have been privacy laws limiting the use of personal data. Due to the rise of social media, other online platforms, mobile applications etc. – all relying on the processing of large amounts of personal data – these laws became outdated and were no longer equipped to provide sufficient protection for individuals and their personal data. Therefore, these national laws were replaced by the General Data Protection Regulation (GDPR), applying in the entire European Union

The GDPR obliges anyone who is processing personal data to comply with the rules of the regulation, that also includes schools and teachers. With children spending a significant part of their time on social media and schools being important collectors of personal data (about their staff and students and online as well as offline), this module is of great importance. Privacy and data protection

are fundamental rights for everyone. It is important that youngsters know about the GDPR and are aware of their rights and obligations in this regard. Since teachers are often a first point of contact for students, they are in a key position to inform and raise awareness about the GDPR amongst students.

**Number of hours: 2**

---

## **Learning Outcomes**

---

- Making both students and teachers aware of and familiar with the GDPR and its aim and importance;
- Knowledge of the obligations for companies and organizations regarding the processing of personal data under the GDPR;
- Knowledge of their own rights in respect of the processing of their personal data;
- Understanding of the concept and value of ‘personal data’ and ‘processing’;
- Creating a natural reflex with students to reflect, before sharing personal data, on whether the information they intend to share is not too personal and constitutes a risk to their privacy;
- What can be found/should be found in a privacy policy;
- The ability to make use of the privacy settings of their social media platform in order to ensure that only people of their choice can see the information on their profile;
- Understanding targeted advertising;
- Knowledge on the part of schools and teachers on how to lawfully make use of social media;
- Knowledge on what to do in case of unlawful use of personal data;

# Training Material

---

## Context

### 1.1. What is the GDPR?

---

The General Data Protection Regulation came into force on the 25<sup>th</sup> of May 2018 and applies to any organization established in the EU or established outside of the EU but which is processing personal data from people in the EU – this includes schools or any other educational establishments. Through the introduction of new rules, the GDPR aims to give individuals back control over their personal data by limiting the way other people and organizations can use your personal data.

The GDPR protects your personal data from the moment you share this data with others. Others are not simply allowed to share, save, copy, link... this data. The GDPR sets out rules for companies, organizations and governments to be followed in case they would like to make use of personal data of individuals: processing must be done lawfully, fairly and transparent. Additionally, the GDPR establishes a number of rights to help individuals to remain in control over their personal data.

Since sharing personal information on social networking sites, or exchanging personal data for access to apps and other web-based services is commonplace nowadays, this module will focus on the GDPR and data protection in light of such services.

### 1.2. What is personal data?

---

#### 1.2.1. In general

Personal data is any sort of information disclosing something about you personally.

E.g. name, identification number, date of birth, address, location data, photos or videos of a person, religion, IP-address, browsing history, marks, behavior slips, social media profiles (including your likes, shares and friends) etc.

This is to be interpreted very broadly: if it is possible to identify an individual directly or indirectly from the information concerned, then that information is personal data.

- Direct identification:

The information allows you in itself to identify the person this information relates to.

E.g. name, phone number, identification number, home address, e-mail address, location data, voice recordings, etc.

- Indirect identification:

The information, as such, is not enough to identify a person, but taking into account additional information – that is already available or that needs to be obtained from another source – does allow you to identify the person concerned.

E.g. license plates can be considered to be personal data, regardless of the fact that you yourself do not have access to databases linking license plates to car owners. The fact that other people can make this connection is sufficient to qualify this information as personal data. The same reasoning applies to information collected by cookies, digital IDs and MAC and IP addresses (which are unique to a device).

One single piece of information (e.g. hair colour, occupation, car...) might not be able to identify a natural person as such, but this can be different when this data is combined with other data. Companies that collect multiple types of data on people (e.g. social media) should take this into account.

Personal data
Information relating to a <u>natural person</u> <b>Not</b> information on companies and other organizations, deceased persons, pets, objects etc.
The <u>format is irrelevant</u> : text, image, video, sound etc.
The information allows to identify a single person, either <u>directly or indirectly</u> (by taking into account additional information)

### 1.2.2. Special categories of personal data

The GDPR distinguishes between ‘regular’ personal data and special categories of data. Due to the sensitive nature of the latter and large potential to negatively affect someone’s privacy and other fundamental rights and freedoms (e.g. the right to not be discriminated) when being used, this type of personal data is, in principle, prohibited from being processed.



### 1.2.3. Why is personal data valuable?

Personal data is often called “the oil of the internet” and the new currency of today’s digital world. In other words, personal data is deemed to be extremely valuable. Many companies offer their online services free of charge, while they earn their money from advertising. It advertising which predominantly benefits from personal data processing.

When you go online, you leave digital footprints. The state of today’s technology allows companies to use and store the personal data you generate when buying certain goods or services, or just by looking for certain things or information (your name, your interests, your wishes, your style etc.). A number of clicks and likes on social media (e.g. Facebook) are enough for companies to conduct an analysis to determine your exact preferences. By combining all this information from different sources, companies are able to paint a clear picture of you. This is where you see the value of personal data, if a company knows what you are looking for or what you are interested in, they are

able to specifically send you advertisements for these products or services. (*More about this under 4. Targeted advertising*)

Personal data is not only interesting to companies, but also to hackers! In the last few years, several big companies made the news in light of hacking scandals, in the event of which personal data of their customers were stolen (e.g. Cambridge Analytica, Facebook, Mastercard).

Finally, personal data also provides interesting information for public authorities, as they can allow them to gain new insights on individuals or groups of individuals.

An uncontrolled use of personal data, however, could put private companies, hackers and public authorities in a position of power.

### 1.3. What is processing?

---

The rules of the GDPR only apply to processing of personal data.

Processing = any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.

E.g. collecting, recording, organizing (e.g. making a mailing list), structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available (e.g. posting a message or picture on the Facebook page of an organization), aligning or combining, restricting, erasing or destructing personal data.

If one of the aforementioned actions are carried out on your personal data, the GDPR applies.

Important to note is that processing for purely personal or household activities does not fall under the GDPR. (e.g. parents taking pictures of their child and schoolmates at a school event to be kept at home in a photo album).

## 1.4. Who has to follow GDPR rules?

---

The GDPR applies to a company or entity (i.e. natural or legal person, public authority, agency or other body), irrespective of their size, sector, number of employees or turnover, 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);
- is established outside the EU and is processing personal data in light of offering goods/services to individuals in the EU, or in light of monitoring the behaviour of individuals in the EU.

Such companies or entities are seen as the controllers of your personal data and need to ensure that the GDPR is respected.

## The rules

### 2.1. The GDPR principles

---

Any company or entity processing personal data will have to follow certain rules.

#### 2.1.1. Lawfulness, fairness and transparency

##### (a) Lawfulness

When a company or organization wants to process your personal data, before doing so, it needs to make sure that his processing can be based on a justification ground – a **lawful basis** – under the GDPR. A lawful basis is a reason for the processing that is determined and accepted by the GDPR (see article 6 of the GDPR).

The most relevant of these lawful bases in light of social media are: personal data processing is necessary **to perform a contract**, the company or organization has obtained your **consent**, or the company or organization has (a) **legitimate interest(s)** in processing your personal data.

##### Contractual necessity

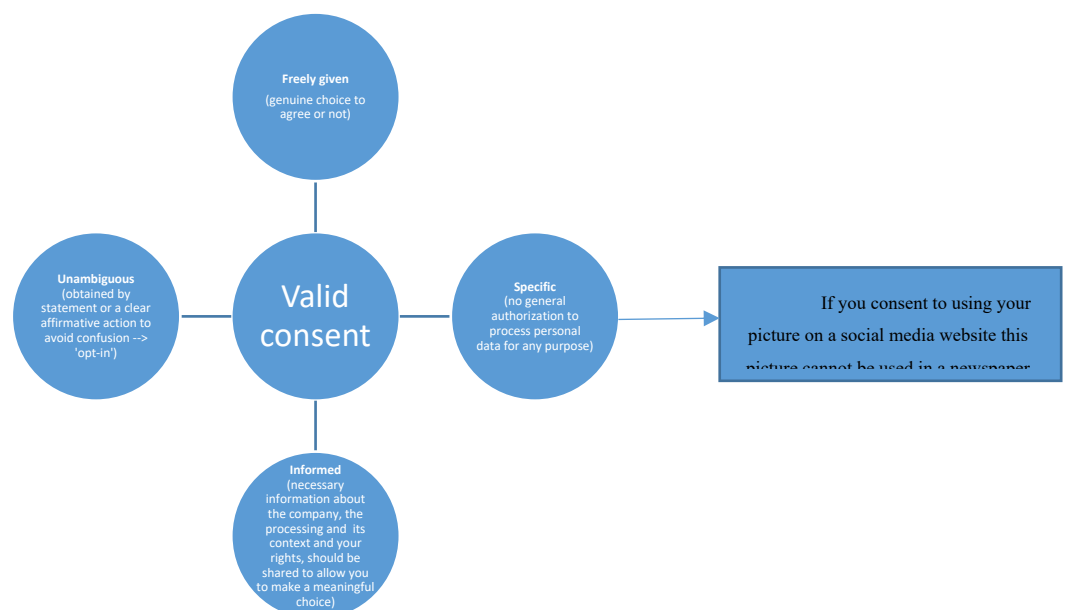


When a company or organization needs to process personal data to comply with contractual obligations between itself and you, or to carry out pre-contractual requests from your side, it can rely on the lawful basis “contract”. Some contractual obligations simply cannot be performed without collecting and processing certain personal data. Processing which is useful, yet not objectively necessary, for performing the contractual service or for taking relevant pre-contractual steps are not covered by this lawful basis.

Example: Twitter processes your personal data – such as, name and e-mail address – in order to create your account, for authentication purposes and to allow for content creation.

## Consent

Consent has a particular meaning under the GDPR. To be valid, consent needs to be:



You should be able to withdraw your consent at any time. Information on how to do this should be provided at the moment you are asked to consent to a certain processing activity. The manner to withdraw consent should be equally easy as giving consent and should not lead to any negative consequences for you (e.g. a fee or lower service levels).

Example: Facebook has a facial recognition feature which allows the social networking site to recognize you in photos or videos on its platform. The use of such a feature entails processing of personal data, namely photos or videos of you. To activate this, Facebook asks for your consent.

The same goes for the ‘location history’ function Facebook offers. When you consent with the use of this function, your location data are being processed in order to explore what is going on around you, to show you relevant advertisements, to look for friends in the area.

Example: Twitter processes information they collect from you on Twitter, your other activity online, and data from their partners in order to show personalized advertising on and off Twitter, based on your consent.

A company or organization 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 children’s consent directly from them can vary from 13 up to 16 years per EU country. (You can check this with you national data protection authority)

### Legitimate interest

The legitimate interests for which it is **necessary** to process personal data, can be your own interests or the interests of third parties (e.g. commercial interests, individual interests or broader societal benefits). This interest needs to be specified in the privacy policy.

To validly rely on this processing ground, companies or organizations must process your data in a way you would reasonably expect, without causing you unwarranted harm. If this is not the case, your interests are likely overriding the ones of the company or organization, which means they are not allowed to process your personal data (on this lawful basis), unless there is a compelling justification for the processing.

Example: Twitter makes inferences about your account – such as interests, age, and gender – in order to provide features such as account suggestions, advertising, recommendation, timeline ranking etc.

Example: YouTube (Google) processes your personal data for their legitimate interests and those of third parties, while applying appropriate safeguards that protect your privacy. This is for example the case for customizing their services to provide you with a better user experience,

marketing to inform users about their services, but also to provide advertising, which keeps many of their services free. (When ads are personalized, they ask for consent.)

### Special categories of data

Important to add is that for special categories of personal data, there are 10 exceptions to the general prohibition to process such data (see article 9 of the GDPR). If one of these conditions is met, special categories of data can lawfully be processed. The most important exception in light of social media is when there is **explicit consent** from the person whose personal data is concerned.

These exceptions form an additional layer of conditions on top of the usual rules. In practice, this means that when you want to process special categories of data, there needs to be a lawful basis (art. 6) and an exception must be applicable (art. 9).

Example: Google asks for your consent before sharing personal information outside of the company. Let's say you make a restaurant reservation through 'Google Home', your permission will be asked before sharing personal data (e.g. name, phone number) with the restaurant. When it concerns sensitive personal information (e.g. allergies), they commit to asking explicit consent.

#### (b) Fairness

The company or entity processing your personal data should do this in a fair manner, which means in ways you could reasonably expect and not in a way which causes unjustifiable negative effects or is misleading to you.

#### (c) Transparency

This is a very important principle, which is linked to fairness! From the start, companies or organizations must be clear, open and honest with you about how they will use your personal data. This requires information to be provided in an easily accessible and understandable language. This is where the privacy policy comes in. Lengthy, complicated privacy policies should be avoided according to the GDPR.

### A privacy policy

The privacy policy is the place to go when you want to obtain information about how your personal data is being collected, used and protected by social media (or any other website). Every privacy policy must contain a large number of mandatory mentions:

- name and contact details of the company/organisation
- contact details of the data protection officer, if they have one
- their purpose(s) for processing personal data and on which lawful basis they rely to process data
- the legitimate interest for the processing (if applicable)
- the (categories of) personal data obtained (if not obtained directly from you)
- the (categories of) recipients of the personal data (will the personal data be shared with other parties?)
- the details of transfers of the personal data to any third countries or international organisations (if applicable)
- how long data is kept (retention period)
- the rights which can be exercised by you (e.g. right of access, right of forgetting, right of rectification, etc.)
- the right to withdraw consent (if applicable)
- your right to file complaints with the data protection authority
- The source of the personal data (if the personal data is not directly obtained from you)
- The details of the existence of automated decision-making, including profiling (if applicable).

### 2.1.2. Purpose limitation

The principle of purpose limitation means that companies or organizations must clearly define a specific purpose for each of their processing activities, before starting. This requirement aims to provide transparency, predictability and user control. Any processing of personal data must be done for a specific well-defined purpose or for additional, specified, purposes that are compatible with the original one. The processing of personal data for undefined and/or unlimited purposes is thus unlawful.

Every new purpose for processing personal data which is not compatible with the original purpose must have its own particular lawful basis and cannot rely on the fact that the data were initially acquired or processed for another legitimate purpose.

Example: If you grant Facebook consent to use the facial recognition feature in order to spot pictures and videos on the platform with you in it, this does not mean that Facebook can use this data for the purpose of providing you with targeted advertisements based on this personal data. It will need a separate lawful basis (e.g. consent) for this.

### **2.1.3. Data minimisation**

Companies and organizations can only process personal data they actually need to achieve their specified purpose, not more. This means that they will regularly have to review the data they store in order to delete anything they don't need.

### **2.1.4. Accuracy**

Companies and organizations need to take reasonable steps to make sure that the personal data they hold is correct and not misleading. This implies that they will have to keep the personal data updated, by correcting or deleting data, where necessary.

### **2.1.5. Storage limitation**

Personal data cannot be kept forever. Companies and organizations must delete or anonymize personal data as soon as they no longer need it to achieve the purpose(s) for which the data was collected. Companies and organizations need to think upfront about how long they want to keep your personal data and whether this time period is justifiable, which will depend on their purposes for processing. Information on this should be entailed in privacy policies.

### **2.1.6. Integrity and confidentiality (data security)**

Protection of personal data against unauthorized or unlawful processing, accidental loss, destruction or damage is a the core of this principle of integrity and confidentiality (data security). The data security principle aims to avoid negative effects to you by obliging the implementation of technical (e.g. encryption, pseudonymisation) and/or organizational measures (e.g. making sure that personal data is not available to everyone within an organization, but only to those how have to work with the data).

### 2.1.7. Accountability

The accountability principle requires that companies or organizations take up responsibility for what they do with your personal data and how they comply with the GDPR. In light of this, they need to put in place measures and records that allow them to demonstrate compliance when asked to do so.

## Your rights

In today's digitalized society it is important to know your rights from a data protection point of view.

### 3.1. The right to be informed

---

Companies and organizations must inform you about the collection and use of your personal data. This is linked with the transparency principle underpinning the GDPR. See 2.1.1.(c) on what information should be given.

The information should be communicated:

- at the time you collect their personal data from them.
- at the latest one month after obtaining the data, in case they received your personal data from someone else.

The information should be concise, transparent, intelligible, easily accessible, and it must use clear and plain language. This information is mainly provided via a privacy policy.

### 3.2. The right to access

---

You have the right to access your **own** personal data, held by a company or organization. In practice, this means that you will receive the following information:

- Whether or not the company or organization is processing your personal data
- A copy of that data (generally, free of charge)

- Additional information: companies or organizations have to provide you with the same information that is required to be in a privacy policy (See 2.1.1.(c)).

Exercising this right helps you to understand how and why companies or organizations are using your data, and to verify whether they are doing in conformity with the GDPR.

It is possible for the company or organization to refuse access when the request is manifestly unfounded (e.g. clearly only done to harass the company) or excessive (e.g. it overlaps with other requests). The reasons for the refusal should be clearly communicated to you. Companies and organizations have one month to respond to the request.

### 3.3. The right to erasure (“the right to be forgotten”)

The GDPR grants you the right to have your own personal data erased. This right is linked to the principles of data minimisation and data accuracy, forcing companies and organizations to consider to delete personal data on certain occasions. You can exercise your right to erasure when:

- your personal data is no longer necessary for the purpose for which it was collected by the company or organization;
- When the company or organization is relying on your consent as lawful basis for holding the data, and you want to withdraw your consent;
- When the company or organization is relying on legitimate interests as lawful basis for processing, you can object to the processing of your data, and if there is no overriding legitimate interest to continue this processing your data will be erased;
- When the company or organization is processing the personal data for to send you direct marketing and you object to that processing;
- When your personal data was processed unlawfully (= without correctly relying on a valid lawful basis);
- When there is a legal obligation obliging the erasure of your personal data;
- When your personal data was collected from you when you were a child in order to offer online services.

There is a particular emphasis on the right to erasure if the request relates to data collected from children. If consent for the processing of personal data was originally given when you were a child

(not fully aware of the risks), it can be very important to be able to withdraw your consent and have the personal data removed. *(Probably every student can think of something they posted online in the past, which they no longer agree with or find embarrassing today)*

The company or organization is not obliged to always (wholly) grant your request as in some cases the right to erasure does not apply (e.g. if the processing is necessary to comply with the law or when processing takes place for archiving purposes in the public interest or for scientific or historical research in case of which the erasure would lead to serious impairment to the research). A company or organization can also refuse the exercise of your right to erasure when the request is manifestly unfounded or excessive (see 3.2).

A remark that should be made here is that even with this right to be forgotten, it will be very difficult (maybe even impossible) to delete your personal data completely from the internet. This is because data is often (un)lawfully shared by companies and organizations with other parties who then again share this data with other parties and so on.

### 3.4. The right to rectification

Based on the right to rectification, you can fix any errors in your personal data held by companies or organizations: inaccurate personal data can be rectified and incomplete data can be completed. This right is clearly linked to the principle of accuracy which companies and organizations need to take into account.

Again, companies and organizations do not always have to comply with your request. If they believe your personal data is accurate, they need to tell you this and explain their decision. Another reason for not (wholly) granting your request to rectification could be when your request is manifestly unfounded or excessive (see 3.2).

### 3.5. The right to restriction of processing

This right is an alternative to requesting the erasure of personal data, it allows you to require the company or organization to stop processing (some of) your personal data usually only for a period of time, while other challenges are being resolved. The right implies that the company or organization can only store your personal data, without further using it.



Companies and organizations also have the ability to refuse the request to restrict processing, under the obligation of providing an explanation for this. One of the reasons for refusal can again be the fact that the request is manifestly unfounded or excessive (see 3.2).

### 3.6. The right to data portability

This right grants you the ability to obtain and move your personal data – that you provided to the company or organization – elsewhere. In practice this means that you can easily move, copy or transfer your own personal data from one IT environment to another in a safe and secure and commonly used manner, or you can ask the company or organization to do this.

This right only applies when the company or organization is relying on ‘consent’ or ‘contractual necessity’ as a lawful basis for processing this personal data, or when they are processing by automated means (i.e. by means of specialised IT programmes and tools and for example not on paper).

Companies and organizations also have the ability to refuse the request to restrict processing, under the obligation of providing an explanation for this. One of the reasons for refusal can again be the fact that the request is manifestly unfounded or excessive (see 3.2).

### 3.7. Right to object

The right to object is not a general right. You can invoke your right to object to your personal data processing based on your particular situation and to data processed for the purpose of providing you with direct marketing. This allows you to stop or prevent companies and organizations from processing (part of) your personal data.

The right to object to processing for direct marketing purposes is an absolute right, which means companies and organizations always have to grant this request. When the right to object is exercised for another reason, companies and organizations may decide to keep processing your personal data if they can prove that there is a compelling reason for them to do so. Companies and organizations also have the ability to refuse the request to restrict processing, under the obligation of providing an

explanation for this. One of the reasons for refusal can again be the fact that the request is manifestly unfounded or excessive (see 3.2).

### 3.8. The rights related to automated decision making, including profiling

Profiling refers to the evaluation of your personal aspects in order to make predictions about you.

Example: A social media website assesses certain information about you (such as your age, sex, height) and based on that classifies you in a certain group for content recommendation or advertising reasons.

Decision-making based solely on automated means refers to the situation where the technology itself takes decisions about you by technological, without any human involvement. This can be done without profiling.

Based on the GDPR, you have the right not to be subject to a decision based on solely automated means, if the decision results in legal effects (i.e. your legal rights are impacted) concerning you or significantly affects you in a similar way (i.e. it influences your circumstances, behavior or choices). Since such decisions likely have a significant impact on your lives (they can relate e.g. to creditworthiness, e-recruitment, performance at work) special protection is necessary.

Example: Insurance companies analyzing social media posts of (potential) clients by using an algorithm looking for certain words and phrases indicating cautious behavior or being healthy to assign a risk level to you in order to decide on the insurance premium.

### 3.8. Practical

When exercising your rights, companies and organizations have one month to respond to your requests and to provide information to support their decision. Requests should be filed with the company or organization, verbally or in writing (usually through an email or a specific section of the

website). It should be as easy to exercise these rights as it was to provide your personal data in the first place.

## Targeted/behavioural advertising

In the past, companies mainly invested in television and radio advertising. A disadvantage of this is that everyone is presented with the same advertisement, whether it of interest to people or not, which is not very efficient. Nowadays, social media and advancements in technology allow for companies to choose to advertise their products and services to consumers in a targeted way: for instance, an ad for running shoes is only presented to social media users who regularly go for a run, and on days when it is not raining. Such targeted advertisements can be found on your social media news feed or on the side of it, and can be recognised by words such as 'sponsored'.

Which of your data is used for advertising?

1. The personal data you enter when creating your social media account (e.g. age, where you live, date of birth)
2. Whatever you post on your social media account, such as photos, videos and comments. E.g. if you post something like 'I am soooo hungry right now', it is possible that you receive an advertisement from a fast food chain;
3. Things you do and look for outside of the social media platform. For instance, if you visit the website of a certain event, you might receive advertisements about this event or a similar event on your social media account. The latter is made possible by 'cookies'.

Cookies are small files stored on your computer, laptop, smartphone or tablet in order to keep track of the websites you are visiting. Note that companies need to ask for your permission before using advertising cookies (there are other types of cookies too). If you do not wish to be tracked across different websites online, you should remember to refuse cookies. The use of cookies and other tracking technologies is regulated under the ePrivacy rules, not the GDPR.

Important to add here is that some social media companies own multiple platforms and, hence, they can use information obtained about you on both platforms (Facebook and Instagram for example);

4. Your (real-time) location. Social media platforms can even see where you are, based on the wifi and gps-tracker on your phone. This could result in you receiving advertisements for a certain gym, if you were in close proximity to it.

All of the information mentioned above, is remembered and interpreted by algorithms and of course not actual human beings. Based on this data, companies who choose to advertise on social media can choose a ‘target group’ (e.g. 16 year-old boys in the area of Amsterdam who like football). The right advertisement, at the right time and in the right place, can seriously influence your behavior, which benefits companies. Although personalized advertising should not always be perceived as a bad thing, you should really be cautious about it. Especially when sensitive data are involved (e.g. race, political preferences etc.), this type of advertising could be tricky and your personal data could even be misused (e.g. targeting you with content that is false, in order to change or radicalize your political preferences).

## What to do in case of infringements?

Did someone unlawfully share your personal? Create a fake social media profile of you? Or, maybe you tried to exercise one of your GDPR rights, but are not satisfied with the reply of the company or organization’s? First, you can always ask the person infringing your data protection rights, to delete or correct the personal data concerned (e.g. a picture, fake profile, contact details). If nothing happens, you could address the social media platform in order to delete or correct the personal data. If these steps are not satisfactory, you can file a complaint with your national data protection authority. (Another option is to enforce your rights through a judicial remedy.)

Every EU country has its own data protection authority. You can find a list here: [https://edpb.europa.eu/about-edpb/board/members\\_en](https://edpb.europa.eu/about-edpb/board/members_en)

Data protection authorities are independent public authorities that monitor and supervise whether companies and organizations within their territory are correctly applying the data protection rules. They also provide expert advice on data protection issues and handle complaints from people

like you. The authorities can issue warnings, reprimands, a temporary or definitive ban on processing and (very high) fines.

On the websites of these data protection authorities you can find how you can file a complaint, this can be via phone, e-mail, or through a contact form available on their website.

## Resources

- [https://fra.europa.eu/sites/default/files/fra\\_uploads/fra-coe-edps-2018-handbook-data-protection\\_en.pdf](https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf) (General handbook on data protection)
- <https://www.youtube.com/watch?v=XVBHishpew8> (YouTube video: what is the GDPR?)
- [https://www.youtube.com/watch?v=3fuirT\\_PwDI](https://www.youtube.com/watch?v=3fuirT_PwDI) (YouTube video: GDPR explained)
- <https://www.youtube.com/watch?v=PVaVIOJniSQ&t=6s> (YouTube video: my data, my choice)
- [https://cris.vub.be/files/27962258/arcades\\_teaching\\_handbook\\_final\\_EN.pdf](https://cris.vub.be/files/27962258/arcades_teaching_handbook_final_EN.pdf) (Free university of Brussels (VUB): The European Handbook for Teaching Privacy and Data Protection at schools)
- [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/747620/Data\\_Protection\\_Toolkit\\_for\\_Schools\\_OpenBeta.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf) (UK GOV: Data protection: a toolkit for schools)
- <https://www.gdpr.school/free-resources/> (useful GDPR sources for schools)
- [https://edpb.europa.eu/about-edpb/board/members\\_en](https://edpb.europa.eu/about-edpb/board/members_en) (List of national data protection authorities)
- <https://ico.org.uk/> (Website UK data protection authority → a lot of information!)
- <https://en.mediawijs.be/poster-step-by-step-how-should-i-protect-my-privacy-on-social-media> (Mediawijs website „How do I protect my privacy on social media?“)
- [https://www.youtube.com/results?search\\_query=internet+safety+tips+for+teens](https://www.youtube.com/results?search_query=internet+safety+tips+for+teens) (YouTube video with internet safety tips for teens)
- <https://www.youtube.com/watch?v=yrln8nyVBLU> (YouTube: Safe Web Surfing: Top Tips for Kids and Teens Online)
- <https://mediawijs.be/nieuws/slag-gdpr-jouw-klas> (Mediawijs website about using the GDPR as part of your classes → in Dutch)



## Extra sources

- <https://d1afx9quaogywf.cloudfront.net/sites/default/files/Resources/School%20College%20Personal%20Data%20Advice%20and%20Guidance.pdf> (Information for schools to be GDPR compliant)
- <https://www.youtube.com/watch?v=xtLR0Ey5-vo&t=76s> (YouTube video with information for schools to be GDPR compliant)
- <https://www.youtube.com/watch?v=SpjpxspJNew&t=7s> (YouTube video with information for schools to be GDPR compliant)



## Learning Snacks

### Raising GDPR awareness is crucial

It is essential that in today's digital age students and teachers and all other staff of educational establishments are aware of GDPR and data protection legislation in general. The amount of personal data floating around online is enormous and will only continue to grow, therefore everyone needs to learn how to handle their and others' personal data in a responsible way.

### Why is the GDPR important? The value of personal data!

Nowadays, we all produce huge amounts of personal data on a daily basis, especially online (e.g. by posting pictures, videos or status updates on social media, but also by online shopping, reading an online newspaper or playing online games – this all generates data that can be linked to you). Some companies – besides collecting and processing personal data to deliver a specific service – aim to collect as much data as possible to effectively target you with advertising. Personal data thus has an important economic value to companies and organizations. Moreover, public authorities are interested in personal data as it can provide them new insights. But also people with malicious intentions such as hackers and identity thieves are out for your data. An uncontrolled use of personal data could consequently put private companies, hackers and public authorities in a position of power and put you in an undesirable situation.

### Think before you share

Always think carefully about what personal data you share with whom and how you want to portray yourself in social media posts (text, pictures, videos). It is important to think in the long term here because the information might be floating around the world wide web forever as it is not easy to delete information from the internet. Take care of your privacy settings so that people you do not know cannot see (much of) your personal data. Even by exercising the right to erasure, you will most likely not be able to wipe out all your digital traces.

## Can I give my own consent for processing my personal data?

There is a legal age for children to be able to consent (or not) themselves to the processing of personal data by providers of online services. This age limit can vary between 13 and 16 years old in each EU Member State.

## Transparency/information is key

One of the main principles underlying the GDPR is the transparency principle: companies and organizations need to be clear about the fact that they process your personal data, which personal data they process, for what reasons and how they do so, for how long etc. This principle is translated into the right for persons to be informed, which should allow you to make informed choices about your personal data. This way the GDPR wants to put individuals in charge of what happens to their personal data.

## How do I know what a company or organization is doing with my personal data?

The first thing you should do when you want to find out what companies or organizations are doing with your personal data is go check out the privacy policy. This policy needs to entail a number of obligatory elements. If there seems to be something missing or something is unclear you can try to contact the company or organizations for further clarifications.

## What to do when someone is misusing my data on social media?

Option 1: contact the person/company/organisation who is using your personal data in an unlawful manner and ask them to delete or correct your personal data.

Option 2: contact the social media platform in order to request the deletion or correction of your personal data.

Option 3: file a complaint with your national data protection authority (see their website).

(Option 4: go to court)



## Infographics

See throughout the teaching material + the infographic below.

**What to do when someone is unlawfully using your personal data on social media?**

**1. Contact the person/company/organisation** who is using your personal data in an unlawful manner and ask them to delete or correct your personal data.

**2. Contact the social media platform** in order to request the deletion or correction of your personal data.

**3. File a complaint with your national data protection authority** (see their website).

## Activity plans with students

---

- Start the class by asking whether the students know what persona data is and why they think it is important to protect personal data.
- Let the students check their privacy settings on Facebook (or another social media website): who is able to see what kind of information about you? Afterwards there can be a discussion between classmates who share why they want their settings to be a certain way or if they would like to change their settings.
- Have the students look up the age threshold to validly give consent under the GDPR in your country. This can be done through the website of your national data protection authority.  
See: [https://edpb.europa.eu/about-edpb/board/members\\_en](https://edpb.europa.eu/about-edpb/board/members_en).
- After receiving the information about the principle of transparency, one of the principles central to the GDPR, and the role of privacy policies in this regard, the students could inspect the privacy policy of a social media website of choice to see whether all the obligatory information is in there. Afterwards they can discuss about this amongst each other.
- After explaining to the students that they have certain rights in relation to the processing of their personal data, they could file an 'access request' with Facebook (or another social media website), to see which personal data Facebook holds about them. See: <https://www.facebook.com/help/contact/2032834846972583>.

## Activity assessment

You can easily assess whether students have understood the information about GDPR by applying questionnaires with short questions whose answer is true or false, as in the examples below:

1. A picture showing a person from the back, completely unrecognisable, is never personal data in the sense of the GDPR? (**False**: the picture as such, without any other information, is not personal data but from the moment someone adds this person's name, address, or phone number to the picture, the picture becomes personal data as it is linked to a specific person from then on)

2. Most websites and apps I use process my personal data. (**True**: the purpose of personal data processing can differ. For example, usually the processing of a name and password is necessary for authentication purposes. Often, personal data such as gender, age, interests are processed for marketing purposes).

3. The GDPR does not treat all personal data in the same way. (**True**: the main divide made in the GDPR is between 'regular' personal data and special categories of personal data (e.g. health, sexual orientation, religion). The latter are to be treated with more care due to their sensitive nature (sharing such data entails greater risk because they could more likely lead to undesirable consequences, such as discrimination, exclusion etc.) and that is why, in principle, processing of such data is prohibited. (Criminal offence data and children's data are also subject to a special regime)

4. A school publishes the report cards of each student online to allow parents to compare the results of their child with those of his or her classmates. This is allowed because it is in the child's best interest. (**False**: This is not how it works. For every processing taking place, a company or other organization – including a school –, needs to rely on a valid lawful basis determined in the GDPR. Since this could potentially negatively affect children, the only way a school would be able to do this is when it obtains consent from each child and/or parent.

5. When processing personal data, consent of the person whose data is concerned is always required. (**False**: consent is only one out of a limited list of lawful bases on which companies and other organizations can rely to justify their processing activities (see articles 6 and 9 GDPR). Therefore consent is not always necessary. For each processing activity you should always choose a legal basis for processing, depending on which basis is most suitable for the situation.

6. In the past, you have consented to your picture being posted on a company's social media page and you really do not like this picture anymore. Unfortunately, because you gave your consent to publish the picture in the past, there is nothing you can do about it. (**False:** you can always withdraw your consent, which means the company will have to delete the picture)

7. Some students were photographed in class and provided consent for that photo to be used in the school prospectus. Later on the school decided to share this brochure on their social media pages. This is allowed under the GDPR. (**False:** consent needs to be given in a specific manner and cannot be bundled for multiple purposes. This means that the school should have obtained separate and explicit consent for the use of the prospectus on its social media channels).

8. The main aim of the GDPR is to restrict online advertising. (**False:** in today's digitized society, in which personal data is super valuable, the GDPR aims to give citizens back the control over their personal data by providing them with greater protection and rights + since it directly applies in the entire EU, it harmonizes the 27 different data protection laws).

9. When you save a picture of another person you found on Instagram to your phone, only to show your hairdresser the haircut you would like, the GDPR does not apply. (**True:** the GDPR does not apply to personal and household activities)

10. Personalised/behavioural advertising on social media is only allowed if you have consented to this? (**True:** for advertising based on your browsing behavior, the use of cookies is necessary. In order for websites to store these cookies on your device, your prior consent is necessary, based on the ePrivacy rules, not the GDPR. Moreover, companies should always provide you the opportunity to withdraw this consent).