GDPR QUIZ

SAFETY > 4.2 PROTECTING PERSONAL DATA AND PRIVACY

TARGET GROUP	AGE GROUP	PROFICIENCY LEVEL	FORMAT	COPYRIGHT	LANGUAGE
All, Job seekers, School drop outs	Adults, Elderly citizens, Teenagers	Level 2	Activity sheet	Creative Commons (BY-SA)	English, French

Through this quiz, participants will understand their rights regarding digital identity and personal data general issues surrounding Europe's General Data Protection Regulation. They'll especially know what steps to take if their personal data rights are infringed upon by any entity.

General Objective	Knowledge acquisition, Skillset building
Preparation time for facilitator	less than 1 hour
Competence area	4 - Safety
Time needed to complete activity (for learner)	0 - 1 hour
Name of author	Nothing 2hide
Support material needed for training	Projector (optional)
Resource originally created in	French

WORKSHOP DIRECTIONS

1 Intro

Since 2018, not so long ago, you will have received many emails explaining that various online platforms (Google, Yahoo!, Microsoft, Facebook, etc.) were changing their terms of service to better respect your privacy. Maybe you deleted them without thinking, or read them too quickly, maybe you don't remember, but this is all related to the GDPR. GDPR = General Data Protection Regulation. A regulation is a law, voted on by Europe, which applies to all member states. Every EU country is obliged to apply the regulation. The GDPR has big implications for the management of personal data of European citizens. It is a regulation favourable to users — probably one of the most advanced laws in the world regarding the protection of user data. What then has changed since the implementation of the GDPR— how exactly does it protect users? We will find out by doing this quiz.

***Facilitation tips**:* You could also use this activity as a test to give after several workshops on the subject of personal data. You can also use it as an introductory guide to personal data and digital identity. Adapt it as you like to make an interesting activity! You could for example follow a TV game show format by making several teams, using buzzers, adding music, etc. Use your imagination! You can also display the questions using a projector. For more information on personal data, we recommend you refer to the workshop plan dedicated to it.

2 Quiz

Create teams depending on the number of participants. Ideally you would have two teams of 3-4 people. Ask the questions one by one to each team. The team with the right answer gets one point. The winning team is the one with the most points.

Which of these 4 is not an example of personal data?

1. List of your favourite sports
2. Your shoe size
3. Your favourite meal
4. The distance from Earth to the moon

Answer: **4**. Personal data is any information related to a physical identifiable person. The distance from Earth to the moon is not personal data but an example of public information.

When was the GDPR implemented?

1. May 2018
2. May 2017
3. May 2020
4. May whenever

Answer: **1**. It has already been over two years and various fines have already been handed out to companies who have broken the regulation: Google, British Airways, Uber and many more.

To which of the following situations does the GDPR not apply?

1. Facebook storing personal data of a user living in Dublin
2. The US Postal Service having registered digital data from a user living in Belgium
3. Google storing emails of a user in Stockholm
4. Facebook storing data of my friend Michael in San Francisco

Answer: **4**. The GDPR applies to the data of all users residing within the EU. See Article 3.

Can you sell your personal data to a third party? (For example: selling your browser history on a daily basis for €1)

1. No
2. Yes, under strict conditions — you can withdraw your consent at any moment
3. Yes but only for a limited time
4. Yes, you can even sell a kidney if you want

Answer: 3. It is possible to sell your data for remuneration if you do it on a legal basis comply with article 6 of the GDPR: 'Processing *shall be lawful only if…the data subject has given* ***consent*** *to the processing of his or her personal data*'. However, the text immediately adds an extra important condition, since consent has to be given 'for one or more specific purposes'. As opposed to selling goods which implies only the simple transfer of property, the company that purchases personal data is obliged to indicate one or several precise purposes — what they intend to do with that data. However, this arrangement is precarious and resembles more the establishment of a lease which the the user can withdraw at any moment. This is because the GDPR has it that the individual may withdraw their consent

as easy as they gave it.

Does the GDPR apply to my personal blog?

1. No, I am not a company like Facebook.
2. No, I don't sell my readers' data.
3. Yes, but only on dates of an even number
4. Yes, as a curator and editor of a site, I collect data so I must inform my users.

Answer: **4.** As a curator of a site, you necessarily collect data: IP addresses, connection time, pages visited, names and addresses given in any contact form. As such you are concerned by the GDPR and have obligations towards your readers. When you have user data, you need to respect the GDPR, meaning you need their clear consent. You therefore need to alert them that you are collecting data, which kind of data, for what reasons, and, where applicable, whether third parties have access to their data.

If you have a Twitter, Facebook, Instagram or Snapchat account, you are concerned by the GDPR.

1. No since I don't collect data
2. No: since these are platforms based in the US, my data is not in Europe
3. Yes, because the GDPR concerns all European citizens regardless of where the data is stored
4. Yes but only on dates of even numbers

Answer: **3**. The GDPR applies to you since it applies to the data of all users residing within the EU. In the arrangement of you signing up to a social media platform, it is not you that collects data but the service provider — Twitter, Facebook, Snapchat, etc. Companies operating these services are obligated to allow users to take back their data, to retract their consent, indeed, to respect the GDPR.

An online service provider may negotiate with a user by saying, for example:

'**Our platform does not and will not respect the GDPR. If you wish to use it, you must accept that we will collect your data, use it and sell without informing you of the details**'.

1. Yes, life isn't fair but there you go
2. Yes, you might even say it's fair enough since they warned us
3. Yes but only on uneven numbered dates
4. No — this is blackmail and we shouldn't negotiate with terrorists

Answer: **5**.To be compliant with the GDPR, a service needs to have the **consent** of the user. If there is one thing to remember from this regulation, it is this. Services using your information need to do it via your consent which is **freely given** (without constraint), **specific** (consent per type of data use), **informed** (user should know how their data will be used, by whom and that can withdraw their consent at any moment), and **unambiguous** (nothing hidden or vague). This consent cannot be constrained, as is the case in the question above. The conditions applicable to consent are applied in articles 4 and 7 of the GDPR. Be aware that the requirement for consent is only one of 6 legal bases required by the GDPR for the authorisation of the use of user data. However, this is the legal basis on which the majority of public services are based in order to have access to your data. For more information see here.

In which case is a site or service that collects your data not obliged to comply with the GDPR?

1. For any activity relevant to the search for extra-terrestrial life
2. For any activity related to national security
3. For any activity linked to baton twirling
4. For any activity regarding extreme sport

Answer: **2**. The GDPR makes an exception for any activity related to national security. This actually represents a regression from some national laws that existed prior to the implementation of the GDPR in the EU, for example the France's Online Privacy Law of 1978.

The GDPR regulates the use of personal data and forbids the use of certain kinds of these. The use of which of these types of personal data is forbidden by the GDPR?

1. Data relevant to the food consumption
2. Data linked to geographical movement
3. Data related to electricity usage (how much someone uses per month, how many devices, etc.)
4. Data regarding sexual orientation

Answer: **4**. Article 9.1 of the GDPR specifies the kinds of the data that are forbidden for use: '*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation* ***shall be prohibited***.' However there are a number of exceptions, e.g. in the case of having the user's explicit consent, when it is necessary for one or more of the following: at

the workplace, social security, social protection, protection of a subject's vital interests, in the case of substantial public interest, by a not-for-profit organisation for political, religious or trade union aims, or for data made manifestly public by the data subject.

When a company breaches the terms of the GDPR, what is the maximum fine they may be charged with?

1. €300,000
2. €3,000,000
3. 4% of the global turnover of the implicated company
4. 3 Snickers

Answer: **3**. National laws that existed prior to the GDPR's implementation could not impose very large fines. By indexing sanctions of the turnover rates, the new regulation is able to charge amounts that serve to effectively to discourage large companies from breaching its terms. For example, Google were the first company to be fined in the wake of not respecting the regulation, to the tune of 50 million euros. This was imposed by the French data regulator CNIL, for 'lack of transparency, inadequate experience, and lack of valid consent regarding ad personalisation'. See here for more information. These next questions involve a service we invented for the purposes of the quiz.

The website/app areyouaddicted tells users to what extent they are addicted to their phones.

It displays the number of hours the visitor uses their phone per day. When they install the app, the GDPR obliges areyouaddicted to ask their consent to access the number of hours used. Will the service then be able to make this data accessible to researchers who would use it for their statistics?

1. Yes, it's even a good thing maybe that researchers have the data. In any case the user already gave their permission to areyouaddicted.
2. No, they authorised areyouaddicted to use the data, not for it to be transferred to a third party.

Answer: 2. The GDPR requires **specific** consent. This means that a user's consent must correspond to one determined. They gave their permission to areyouaddicted for it to access the number of hours they use their phones. If the service wants to sell or volunteer the information to a third party, they need to ask the user for explicit permission for this specific usage.

If you refuse to consent that a site may use some of your data, the service will reduce the quality of its service.

1. Yes, a service can encourage a user to give their consent by restoring full functionality for their service if they do.
2. No, that's called blackmail and we don't negotiate with terrorists.

Answer 2. Consent must be given **freely**, meaning it must not be constrained or coerced. The subject must be given a real choice, without needing to undergo negative consequences should they decide to refuse. For example, WhatsApp asked its users for authorisation to use their data for the service to work but also asked them for the data to be accessible by Facebook (the company that owns Whatsapp). If you were to refuse, Whatsapp didn't work. The only way to prevent the harvesting of your data by Facebook would have been to uninstall the app. It has been facing GDPR-related fines in Europe for this and similar practices. See here for more information.

You read the terms of service of areyouaddicted but they are not very clear regarding how your data will be used.

You can't understand whether these will be displayed only on your phone to inform you of your daily usage or if they will be made available to a third party. You would read them completely but there are 152 pages.

1. In these 152 pages, you should be able to find the details of your data use. You are just perhaps a little too dumb to understand, but it must be legal.
2. 152 pages to explain what they will do with your data – that's way too much, they're probably trying to hide or obfuscate something.

Answer: **2**. Those responsible for using your data need to get your **informed** consent. The GDPR requires transparency. A service should make clear to its users:

- the identities of those responsible for using their personal data
- the purpose of its use
- the identity of those who will have access to the data
- the length of the time the data will be kept
- whether the data will be sent outside the EU
- the existence of rights of access, rectification, erasure, limitation and opposition to the processing and the right to data portability

- the existence of the right to file a complaint to an external regulatory body

To get your consent for the use of your data, the areyouaddicted did some of the work for you already: all the boxes are ticked by default on the authorisation form — you just need to give the final nod.

1. Nice, that'll save some time
2. That's not allowed. Some people will go too fast and click 'I agree' without understanding what will be done with their data.

Answer: **2**. Once again, user consent must be secured. This must be specific, freely given, informed and unambiguous. Here the choices are pre-filled. Consenting here is not what we call affirmative, so it is not valid.

You are no longer satisfied with areyouaddicted. You found another app which is much easier to use. You would like to get back your history with areyouaddicted and use it with your new app.

1. No way. areyouaddicted will never bother relinquishing your history as you are leaving.
2. You will figure it out yourself and find all the details manually.
3. areyouaddicted is obligated to give you your data.
4. Whatever, your iPhone X just fell and broke — the screen is broken — can't be bothering about data.

Answer: **3**. The GDPR introduced new laws meaning that users have the right to **data portability**. This means that users are have the right to retrieve their data in an easily readable format. That can then be stored and transmitted easily from one system to another with the aim of being used for personal reasons. This is really your data! This is why services like Facebook and Google have added new options for data retrieval. More information on data portability.

You have authorised areyouaddicted to share my data with third parties for statistical usage. You have changed your mind and no longer want these third parties to have access to your information.

1. Too late: the data is already out there. You gave your consent and there's no way back.
2. No worries, you can contact these third parties individually and ask them to delete your data.
3. You can ask areyouaddicted to delete your data. They have a legal obligation to delete them. They will contact the third parties.

Answer: **3**. The GDPR includes a right to erasure. A user may withdraw their consent at any moment and the service they are dealing with is obligated to delete their data. This is not always as simple as it should be, as evidenced for example by how difficult it can be to really delete a Facebook account.

You just learned that areyouaddicted was hacked almost a year ago and they only informed you now!

1. This is normal — they have so much work and they can't be expected to warn everyone.
2. No worries, it's just user data.
3. This is illegal — they should have informed you as soon as it happened
4. You can't be bothering about this, your iphone 11 just fell and broke.

Answer: **3**. With the GDPR, platforms involved in user data use are legally obliged to inform their users of user data breaches within 72 hours. The GDPR was created so that companies with whom we store personal data become responsible more loyal towards their users. Many data breaches have been observed in recent years. Before GDPR, companies had no obligation either to protect their users' data nor to warn them of a breach. For example, in 2016, Uber had the data of 57 million users stolen. They informed no one – not even the users – and it was only revealed by the media one year later that this happened.

3 Conclusion

In Europe, prior to the GDPR, many countries had data protection acts already established. These generally lacked legislative power in cases where personal data laws were not respected. They could often only give limited fines, as in the case of France's CNIL or Ireland's Data Protection Act (the latter only being able to fine up to €5000 per offence). The GDPR changed all this, as data protection bodies may now fine companies based on their annual turnover, which arguably gives them real power. With the GDPR in Europe, data protection has become normative instead of declarative and this has changed everything. Companies must now be always aware of the GDPR's requirements and be ready at any moment to prove they are compliant. For the user, if there is only one thing to remember about the GDPR, it is that from now on, services responsible for treating personal data are obligated to be loyal to their users. This means getting consent that is freely given, specific, informed and unambiguous. Now

you know what it is!