GDPR

A code watch

What is GDPR ?

- "General Data Protection Regulation"
  - "Règlement Général sur la Protection des Données" (RGPD)
- European law intended to protect its citizens' personal datas
- Voted in 2016, in application since 2018

What are "personnal datas" ?

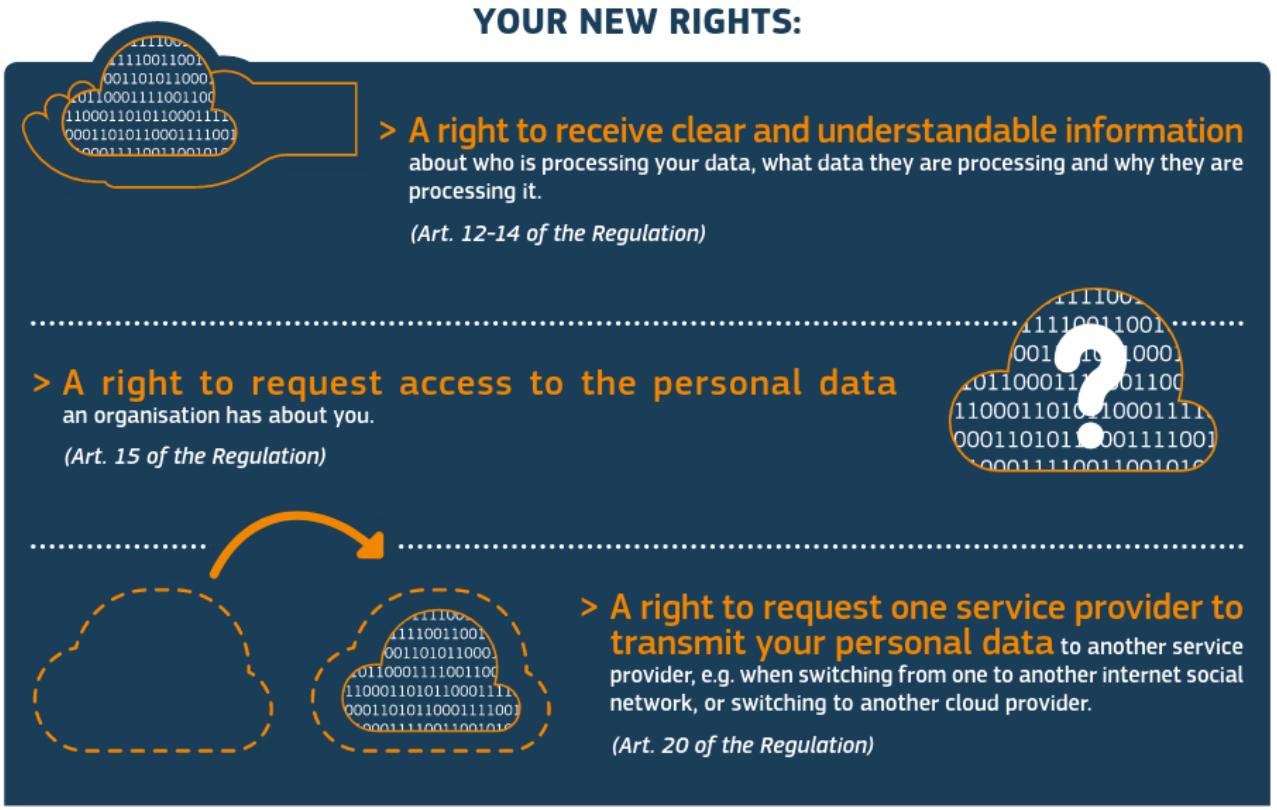
Can be processed

- Name
- Address
- ID card/passport number
- Income
- Cultural profile
- IP address
- Data held by a hospital or doctor (which uniquely identifies a person for health purposes).

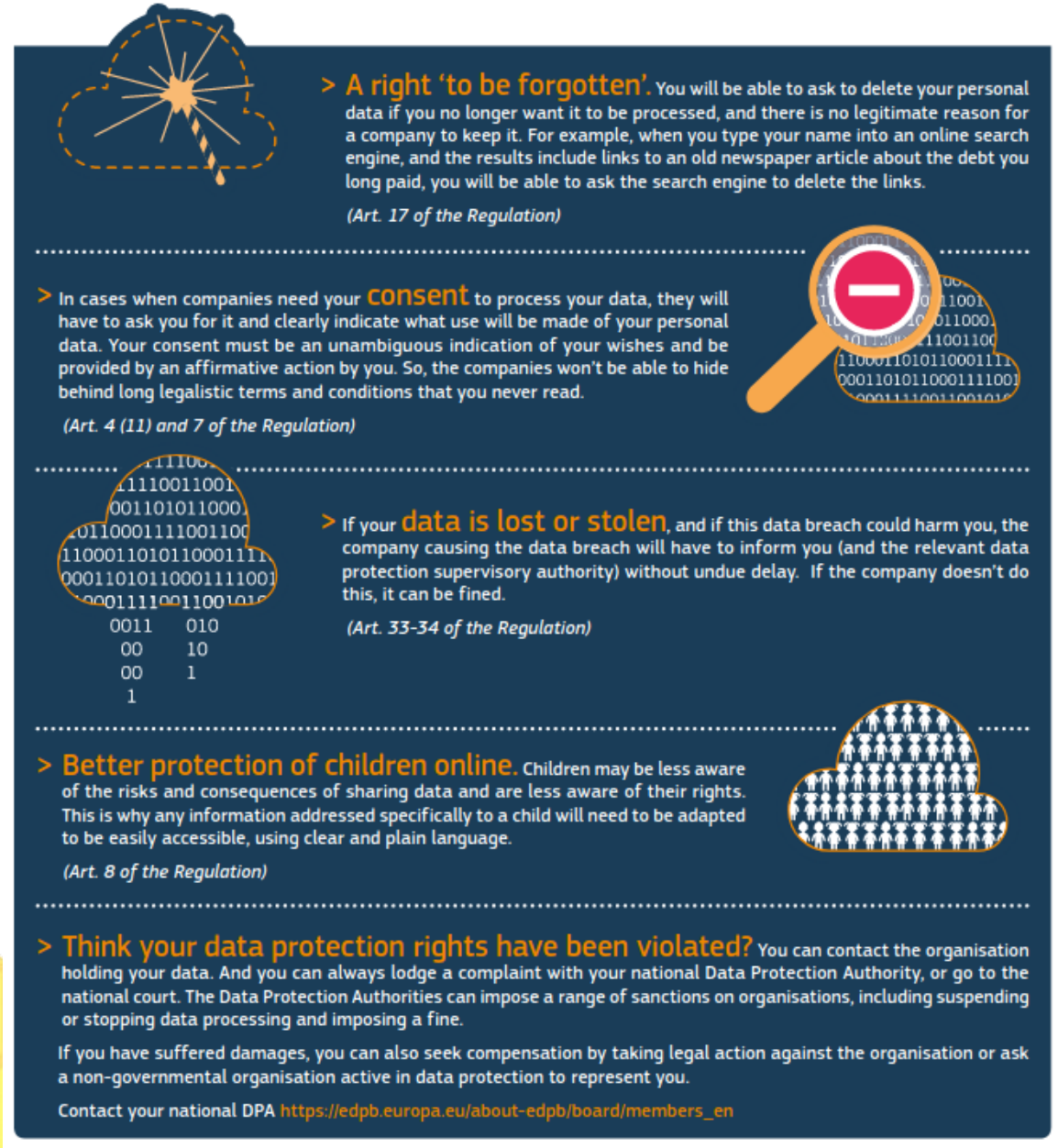
Cannot be processed

- Racial or ethnic origin
- Sexual orientation
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Genetic, biometric or health data except in specific cases
- Personal data related to criminal convictions and offences unless this is authorised by EU or national law

What right does it give to the individuals ?



What right does it give to the individuals ?



> **A right 'to be forgotten'.** You will be able to ask to delete your personal data if you no longer want it to be processed, and there is no legitimate reason for a company to keep it. For example, when you type your name into an online search engine, and the results include links to an old newspaper article about the debt you long paid, you will be able to ask the search engine to delete the links.

(Art. 17 of the Regulation)

> In cases when companies need your **consent** to process your data, they will have to ask you for it and clearly indicate what use will be made of your personal data. Your consent must be an unambiguous indication of your wishes and be provided by an affirmative action by you. So, the companies won't be able to hide behind long legalistic terms and conditions that you never read.

(Art. 4 (11) and 7 of the Regulation)

> If your **data is lost or stolen**, and if this data breach could harm you, the company causing the data breach will have to inform you (and the relevant data protection supervisory authority) without undue delay. If the company doesn't do this, it can be fined.

(Art. 33-34 of the Regulation)

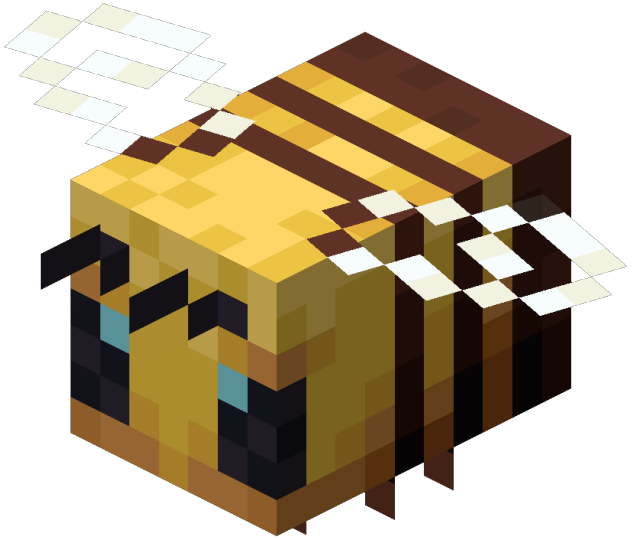
> **Better protection of children online.** Children may be less aware of the risks and consequences of sharing data and are less aware of their rights. This is why any information addressed specifically to a child will need to be adapted to be easily accessible, using clear and plain language.

(Art. 8 of the Regulation)

> **Think your data protection rights have been violated?** You can contact the organisation holding your data. And you can always lodge a complaint with your national Data Protection Authority, or go to the national court. The Data Protection Authorities can impose a range of sanctions on organisations, including suspending or stopping data processing and imposing a fine.

If you have suffered damages, you can also seek compensation by taking legal action against the organisation or ask a non-governmental organisation active in data protection to represent you.

Contact your national DPA https://edpb.europa.eu/about-edpb/board/members_en



Little break : time to forage

To whom and when does it apply ?

The GDPR applies if:

- The company processes personal data and is based in the EU
- The company is outside the EU but processes personal data in EU

The GDPR does not apply if:

- The data subject is dead
- The data subject is a legal person
- The processing is done by a person acting for purposes which are outside his trade, business, or profession

What are the sanctions ?

- Penalty of up to 20 000 000€ or up to 4 % of the turnover
- Up to 5 years of prison
- Suspension of activity or data processing activity
- Some other sanctions that can be determined by the country

Some examples of sanctions :

- Google : 50 000 000 €
- A german hospital : 105 000 €
- Proximus : 50 000 €
- The mayor of Pepinster : 5 000€
- Microsoft : Office 365 banned in german schools

Cloud Act (and Patriot Act)

Back to the hive for the questions !

Sources

- https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-citizens_en.pdf
- https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/indexamp_en.htm
- https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
- https://www.lesechos.fr/tech-medias/hightech/cookies-le-consentement-biaise-des-internautes-1162585
- https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679#d1e6234-1-1
- https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps
- https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la
- https://www.vedia.be/www/article/info/politique/le-bourgmestre-de-pepinster-philippe-godin-condamne-pour-non-respect-du-rgpd_100289_89.html
- https://cyberveille-sante.gouv.fr/cyberveille-sante/1535-un-hopital-allemand-condamne-105-000-euros-damende-pour-non-respect-du-rgpd
- https://www.lecho.be/entreprises/telecom/proximus-ecope-d-une-amende-record-pour-non-respect-du-rgpd/10227851.html
- https://fr.wikipedia.org/wiki/CLOUD_Act
- https://fr.wikipedia.org/wiki/USA_PATRIOT_Act
- https://www.wimi-teamwork.com/fr/blog/cloud-act-patriot-act-proteger-organisation/
- https://donnees-rgpd.fr/donnees-personnelles/cloud-act-anti-rgpd/