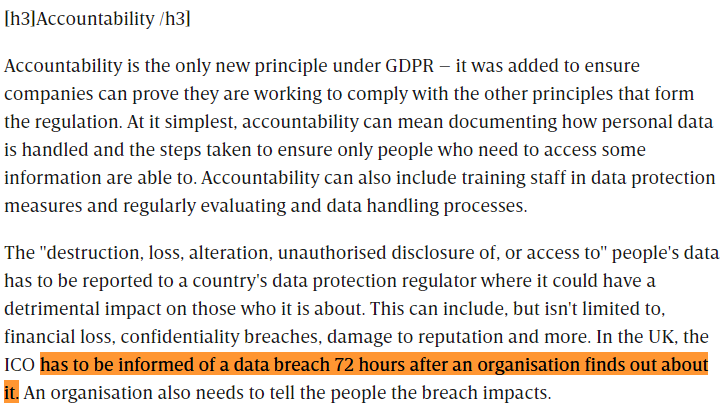
To put GDPR into simple perspective, it’s like a huge rulebook that tells companies like Facebook how they should handle your personal information, otherwise the companies will face big lawsuits. GDPR has the biggest fines out of all major regulation acts, reaching up to 4% of annual global turnover or €20 million, whichever is higher. It’s followed closely by the UK Data Protection Act 2018, what’s basically the same GDPR regulation act, simply adapted more towards the UK, the fines are quite similar to GDPR, reaching up to 4% of annual turnover or £17.5 million.

Now let’s analyze what challenges Facebook faces in regards to GDPR. I will be mostly referring what I’ve researched from <https://www.epc.eu/en/publications/Metas-Pay-or-Okay-Is-this-the-final-challenge-for-EU-GDPR~5672dc> and <https://gdpr.eu/the-gdpr-meets-its-first-challenge-facebook/> with help of chatGPT to summarize my thoughts.

**Accountability:**

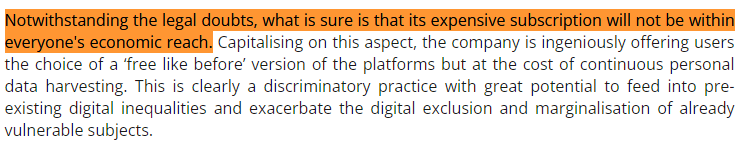
This one is pretty self explanatory, you find a data breach - you inform about it within 72 hours. And Facebook was still not giving any information 4 days after the security breach.





**Transparency:**

In November 2023 Facebook “started selling European users a monthly subscription between €9.99 and €12.99 to experience ad-free products.”



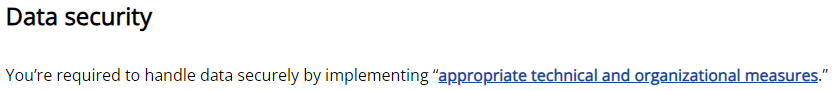
This quote is saying that Facebook might not be very clear about how easy it is for everyone to afford their new subscription plan. It's like saying they might not be telling us clearly if everyone can pay for it or not. This makes it hard for people to know if they can choose the option that protects their privacy without spending too much money, meaning that some people might not be able to get the privacy protection they want because they're not sure if they can afford it.

**Lawfulness:**  
We can see another breach using the same exact quote *“Notwithstanding the legal doubts, what is sure is that its expensive subscription will not be within everyone's economic reach”*

**

If there are legal doubts regarding Facebook’s attempt to add a subscription based model, that means they had no “legal basis” to even try that subscription model, meaning that’s another breach.

**Data security:**



Now while one of the research states that Facebook had *“Repeated data breaches”*  I digged a bit deeper of what’s considered repeated and boy oh boy.. There were “some” breaches, especially in the recent years.  
*1.December 2007: Beacon Advertising Program Allows Facebook User Tracking*

*2.December 2009: Facebook Makes Previously Private User Information Public*

*3.May 2010: Facebook Shares User Data with Advertisers via “Privacy Loophole”*

*4.November 2011: Facebook Settles with FTC on Privacy Charges*

*5.January 2013: Facebook’s Graph Search Rollout Ignites Privacy Concerns*

*6.June 2013: Bug Exposes Personal Data of 6 Million Users*

*7.March 2018: Cambridge Analytica Scandal Affects 50+ Million Users*

*8.May 2018: Facebook Bug Makes 14 Million Users’ Private Posts Public*

*9.September 2018: Attackers Access Data of Up to 90 Million Facebook Users*

*10.December 2018: New York Times Discovers Facebook Sharing User Data Without Permission*

*11.March 2019: Up to 600 Million Facebook Passwords Stored in Plaintext Files*

*12.April 2019: 540 Million Facebook User Records Found on Public Server*

*13.April 2019: Facebook Uploads 1.5 Million Users’ Email Contacts Without Permission*

*14.July 2019: FTC Imposes $5 Billion Penalty and New Privacy Restrictions on Facebook*

*15.September 2019: Data for 419 Million Facebook Users Found on Exposed Server*

*16.December 2019: Hacker Group Captures Data from 300m+ Facebook Accounts*

*17.June 2020: Facebook Accidentally Shares User Data with Developers*

*18.April 2021: Personal Data on 530m+ Facebook Users Leaks in Online Forum*

*19.April 2023: $725 Million Privacy Settlement Opens to Applications*

I’m pretty sure that can easily be called repeated data breaches, meaning they are not taking Data Security strong enough according to GDPR laws.

First and foremost suggestion to comply with GDPR laws would be to be more transparent and report the breaches on time, I believe that’s the easiest way to show at least some level of compliance. And second, being the more serious one would be to invest into cybersecurity more and improve constantly. Of course it’s easier said than done, most likely companies like Facebook already have top tier cyber security, yet there’s always room for improvement and let’s be honest, although Facebook had ups and downs, their 2023 net profit is still close to 80% higher than 5 years ago (2018) - 39bil and 22bil accordingly, so it’s not like Facebook has no budget to allocate towards the security.