Forwards or Backwards

https://forwardorbackwards.com



GDPR and Privacy: How One EU Law Changed the Internet

Watch on YouTube: https://www.youtube.com/watch?v=IxaI8OQy994

You have seen the banner. We value your privacy. Accept all, manage preferences, reject. One European Union law made nearly every company on earth write that - the General Data Protection Regulation, in force since 25 May 2018.

This video explains how GDPR actually works: why the 1995 Data Protection Directive it replaced left enforcement to 28 different national regimes, the legislative path from the European Commission's January 2012 proposal to the law's 2016 adoption, and why GDPR's Article 3 reaches any company on earth the moment it handles a European's data, not just companies based in Europe.

It covers the law's five core principles - lawful basis, purpose limitation, data minimisation, storage limitation and accountability - the rights it gives individuals (access, correction, erasure, portability, objection to automated decisions), and what it demands of companies: real consent, 72-hour breach notification, data protection officers, and fines of up to 4% of global turnover or 20 million euros.

Then the cases that made the ceiling real: CNIL's EUR 50 million fine against Google (2019), Luxembourg's EUR 746 million fine against Amazon (2021), the Irish DPC's record EUR 1.2 billion fine against Meta (2023), and the Dutch DPA's fine against Clearview AI (2024). Then the 'Brussels effect' - how GDPR became the template copied by California, Brazil, the UK and more than 140 countries - and the friction between GDPR's rules on consent and purpose limitation and how AI models are trained on scraped personal data.

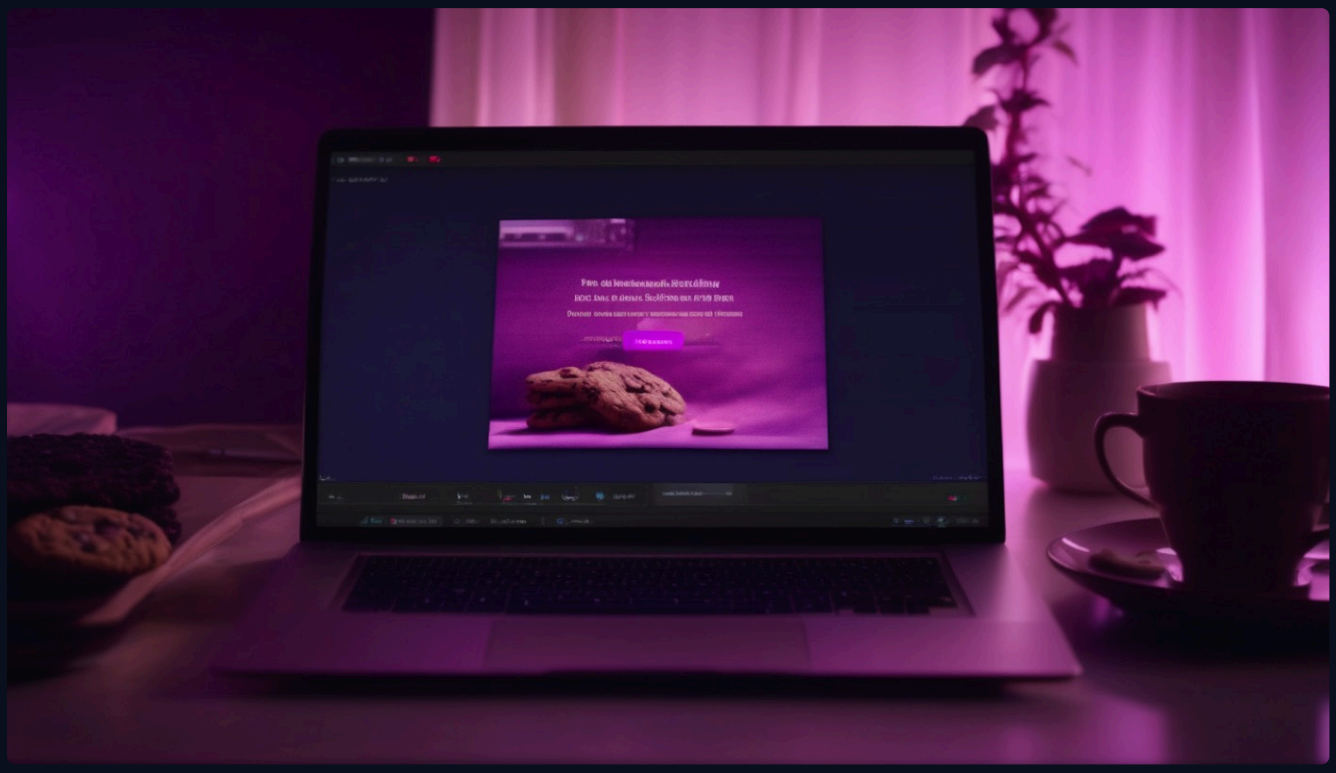
Finally, two live fights: the European Commission's November 2025 Digital Omnibus package, which proposes to loosen GDPR's AI and record-keeping rules and remains stuck in Council negotiation; and the EU-US Data Privacy Framework, upheld by the EU's General Court in September 2025, under appeal to the Court of Justice, and newly in question after a June 2026 US Supreme Court ruling stripped the Federal Trade Commission of its independence.

Every figure is on screen with its source and date.

Chapters

1. A letter from Brussels
2. The directive that wasn't enough
3. From directive to regulation
4. Who the law actually covers
5. The core principles
6. The rights it gives you
7. What it demands of companies
8. The fines that made it real
9. The Brussels effect
10. GDPR meets artificial intelligence
11. The 2026 fight to loosen it
12. The transatlantic question still open

1. A letter from Brussels



You have seen the banner. A box drops over the page: we value your privacy. Accept all, manage preferences, reject.

Or an email arrives from an app you forgot you had installed. We are updating our privacy policy.

One law made nearly every company on earth write those words. It is a European Union regulation, and it reaches a company anywhere, the moment that company handles data belonging to someone in Europe.

That law is the General Data Protection Regulation, usually just called GDPR. It took effect across the EU on the twenty-fifth of May, twenty eighteen.

This video follows GDPR from the failed law it replaced, through the fines that made it real, to the fight now under way in Brussels to loosen it. First, why the old rules were not enough. Then what GDPR actually demands, and the rights it gives you. Then the cases that turned its numbers into real money. Then the question every company training an AI model is now asking.

2. The directive that wasn't enough



Before GDPR, there was a directive. The European Union passed it in nineteen ninety-five, the year most of today's internet giants did not yet exist.

A directive sets a goal and lets each country write its own law to reach it. The nineteen ninety-five directive gave the EU's member states a shared idea of data protection, and just as many different ways of enforcing it.

That gap mattered more as the internet grew. A company based in one country answered to one regulator, even when its service reached every other member state.

In twenty eleven, a Gmail user in Europe sued Google over the scanning of her email. The case did not rewrite the law by itself. But it crystallised a worry that had been building for years. One directive, enforced many different ways, could not govern companies that operated across the whole of the internet.

Within months, European regulators were calling for a single EU-wide law to replace the patchwork entirely.

3. From directive to regulation







That call took four years to become a draft, and four more to become law.

The European Commission, the EU's executive arm, proposed the new law on the twenty-fifth of January, twenty twelve. The European Parliament and the Council, which represents national governments, then spent years negotiating the details between them.

They adopted the final text on the twenty-seventh of April, twenty sixteen. It became applicable, meaning companies actually had to obey it, two years later. That happened on the twenty-fifth of May, twenty eighteen.

Here is why that gap between adoption and application matters, and why the date itself matters. A regulation binds every member state directly, the moment it applies, with no national law needed in between. The directive it replaced never worked that way. Each country had translated it into its own statute, in its own time, which is exactly the patchwork the new law was built to end.

This is the European Parliament's chamber in Brussels, where the text was debated clause by clause.

Both institutions sit a short walk apart, in the same small stretch of the city.

And this is the Berlaymont, the European Commission's headquarters, where the original proposal was drafted.

Two years of warning, and then one law, enforced the same way everywhere.

4. Who the law actually covers



GDPR's reach is the part most people get wrong. It is not a law about companies based in Europe. It is a law about data belonging to people in Europe, wherever the company sits.

Lawyers call this extraterritorial reach, under the law's Article 3. It applies to any organisation, anywhere in the world, that offers goods or services to people in the EU, or that tracks their behaviour. Based in Europe is not the test. Reaching someone in Europe is.

That is why a retailer in California, or a bank in Singapore, or an app studio in Seoul, can all be bound by a European law they never voted on and may never have read.

It works because of leverage, not politics. The EU is one of the largest consumer markets on earth. A company that wants to sell there has to follow the rule that protects the people buying.

5. The core principles



GDPR's rules build on five ideas. None of them is complicated once it is said plainly.

The first is lawful basis. A company needs a legal reason to use someone's data at all. Consent is one, but so is a contract, or a legal duty. No permission, no processing.

The second is purpose limitation. Data collected for one reason cannot quietly be reused for another. If an app collects your address to deliver a parcel, it cannot then sell that address to an advertiser without telling you.

The third is data minimisation. Collect only what the stated purpose actually needs, not everything that might be useful one day.

The fourth is storage limitation. Data should not be kept forever just in case. The fifth is accountability. A company has to be able to show a regulator that it followed all of the above, not merely claim that it did.

6. The rights it gives you



If the law constrains companies, it hands power to individuals. GDPR calls you, formally, a data subject, and gives you rights that did not used to exist in writing.

You can ask any company what personal data it holds on you, and get a copy. That is the right of access. You can have wrong data corrected. And you can ask for your data to be deleted, which the law calls the right to erasure, and which the press nicknamed the right to be forgotten.

There is also data portability: the right to take your data from one service and move it to a competitor, in a format you can actually reuse. And there is the right to object to automated decisions and profiling, when a machine, not a person, has decided something about you.

A request like this follows a fixed path. You ask. The company has one month to answer. If it refuses, or says nothing, you can complain to your country's data protection authority.

That one-month clock is not a courtesy. It is written into the law.

7. What it demands of companies



For companies, GDPR adds up to a list of concrete jobs, not a vague instruction to be careful.

Consent has to be freely given, specific, and as easy to withdraw as it was to give. That is why a cookie banner now needs a reject button as prominent as its accept button. Vague box-ticking no longer counts.

If personal data is breached, the company has seventy-two hours to tell its regulator, and in serious cases, the people affected too. Many companies must also appoint a data protection officer: a named person responsible for compliance, who reports independently of the people whose work they are checking.

For riskier projects, the law requires a data protection impact assessment first. That is a written check of what could go wrong, done before the project launches, not after.

Break the rules badly enough, and the ceiling is four per cent of a company's global annual turnover, or twenty million euros, whichever is larger. That is not a per-incident fine. It is calculated against the whole company, worldwide.

8. The fines that made it real









A ceiling only matters once a regulator actually uses it. Four cases did more to make GDPR real than any amount of legal text.

In twenty nineteen, France's regulator, the CNIL, fined Google fifty million euros, for ad personalisation that ran without clear, specific consent. It was the first fine the world actually noticed.

This is Google's Mountain View headquarters, the Googleplex. The fine landed an ocean away from it, but the rule reached all the same, because the people affected were in Europe, not because the company was.

Luxembourg's regulator fined Amazon seven hundred and forty-six million euros in twenty twenty-one, again over advertising, and again over consent. At the time, it was the largest GDPR fine ever issued, a record Amazon held for less than two years.

This is the Amazon Spheres, part of Amazon's Seattle headquarters. The company is still appealing the fine, though Luxembourg's courts upheld it in full in twenty twenty-five.

Ireland's regulator broke the record again, and for a different reason entirely.

In twenty twenty-three, Ireland's Data Protection Commission fined Meta one point two billion euros, the largest GDPR fine to date, for unlawfully sending European users' data to the United States.

This is Meta's headquarters in Menlo Park, California. The fine was not about advertising at all. It was about where the data physically went, and the legal cover Meta used to send it there.

The fourth case left advertising behind completely. In twenty twenty-four, the Dutch data protection authority fined Clearview AI thirty point five million euros, for scraping people's photographs from the internet to build a facial-recognition database, without asking anyone first.

Four regulators, four very different complaints, and one shared result. The number on the fine was never small enough to ignore again.

9. The Brussels effect



A rule written for one market rarely stays inside it. GDPR became a template almost everywhere else.

Researchers call this the Brussels effect: a market large enough that global companies find it cheaper to meet its toughest rule everywhere than to run two different systems. The EU is one of the largest consumer markets on earth, so companies built GDPR-style systems once, and used them worldwide.

California passed its own privacy law, modelled closely on GDPR's rights of access, correction and deletion. Brazil passed one too, the LGPD, built on the same five principles. And after Brexit, the United Kingdom simply kept GDPR in its own domestic law, renamed UK GDPR.

By one recent count, more than a hundred and forty countries now have a data protection law that owes something to GDPR's template. Most of them were written after twenty eighteen, with GDPR's text open on the drafter's desk.

One European regulation, copied, adapted and re-enacted, until "GDPR-style" became its own category of law.

10. GDPR meets artificial intelligence





GDPR was written for a world of settled databases, not for a system trained once on billions of scraped examples. The two frameworks do not fit together easily.

Training a large AI model usually means scraping huge amounts of text and images from the open internet, much of it written by, or about, identifiable people. GDPR's purpose limitation rule says data gathered for one reason, a blog post or a forum comment, cannot simply be repurposed for another. Training a model is a new purpose, and a new purpose needs its own lawful basis.

The right to object to automated decisions adds a second friction. If a model's output affects someone, a loan decision, a hiring screen, GDPR gives that person a right to a human review, not just the machine's answer. A system trained to replace human judgement runs straight into a law built to guarantee it.

This is a data centre, the kind of building AI models are trained and run inside. The electricity and the hardware are new. The question of whose data is inside the model is the same one GDPR has asked since twenty eighteen.

None of this sits apart from the EU's newer AI Act, which layers its own rules for AI systems on top of GDPR's existing ones, rather than replacing them.

11. The 2026 fight to loosen it



GDPR has not stood still since twenty eighteen. Its toughest critics are now inside the institution that wrote it.

In twenty twenty-five, the European Commission published a package it calls the Digital Omnibus. Among other things, it proposes to let companies train AI systems on personal data under a looser legal basis, and to cut back some of GDPR's record-keeping duties.

Privacy regulators and civil-society groups pushed back hard, arguing the proposal weakens protections the law was built to guarantee. By the middle of twenty twenty-six, member states inside the Council could not agree on a shared position, and the presidency holding the file withdrew its compromise text for lack of support.

As of this video, there is no agreement in sight. The AI half of the package has already become law. The GDPR half remains stuck in negotiation, with no date set for when, or whether, it moves again.

12. The transatlantic question still open





One more fight is still running, and it decides whether European data can keep flowing to American servers at all.

Most European companies send at least some personal data to the United States, into cloud storage, into analytics tools, into AI services. GDPR allows that only if the destination offers protection the EU judges adequate. The current legal cover for sending data there is called the EU-US Data Privacy Framework.

A French member of parliament, Philippe Latombe, challenged that framework in the EU's General Court, arguing American surveillance law still did not meet the EU's standard. In twenty twenty-five, the court dismissed his case and upheld the framework. He has since appealed to the EU's highest court, the Court of Justice, where the case is pending, with a hearing unlikely before late twenty twenty-six.

This is the Court of Justice of the European Union, in Luxembourg, not to be confused with the General Court that ruled first. A final answer on the framework's survival now rests with the judges who sit inside it.

Then, in the United States, something else moved underneath the whole arrangement.

In twenty twenty-six, the US Supreme Court ruled that the president can remove the heads of independent agencies, including the Federal Trade Commission, at will. The Data Privacy Framework had relied on the FTC's independence from the White House as part of its case for adequacy.

The privacy campaigner Max Schrems, whose earlier challenges had already struck down two previous transfer arrangements, reacted within hours. "Even in the European Commission's logic, the basis for any EU-US data transfer deal is dead," he said.

So the law that started as Europe's answer to one country's surveillance habits is now asking whether any one country, including the one that currently does, can credibly promise to protect data on Europe's terms. For a law that rewrote the rules of the internet once, that is not a footnote. It is the live chapter.

Sources and credits

Primary sources

- Regulation (EU) 2016/679 (General Data Protection Regulation), Official Journal of the EU, adopted 27 April 2016, applicable 25 May 2018 - Articles 3, 5, 6, 7, 15-22, 33, 35, 37-39, 83. Standard legislative text.
- European Parliament Legislative Observatory, procedure file 2012/0011(COD) - Commission proposal 25 January 2012; legislative history to 2016 adoption.
- CNIL, deliberation SAN-2019-001, 21 January 2019 - EUR 50 million fine against Google LLC..
- CNPD (Luxembourg), decision fining Amazon Europe Core S.a.r.l. EUR 746 million, 16 July 2021; confirmed by the Luxembourg Administrative Court, 18 March 2025..
- Irish Data Protection Commission, decision on Meta Platforms Ireland Ltd, 22 May 2023 - EUR 1.2 billion fine..
- Autoriteit Persoonsgegevens (Dutch DPA), press release on the Clearview AI fine, 3 September 2024 - EUR 30.5 million..
- CEPA, 'Mapping the Brussels Effect: The GDPR Goes Global', 7 August 2025 - the 'over 140 countries' figure..
- European Commission, Digital Omnibus and Digital Omnibus on AI legislative package and press release, 19 November 2025..
- PrivacyNext, 'Digital Omnibus Negotiations (GDPR)', July 2026 update; aavit.cz, 'Digital Omnibus: Council Negotiations Postponed' - Cyprus Presidency withdrew its compromise text 30 June 2026..
- General Court of the European Union, judgment, Case T-553/23 (Latombe v European Commission), 3 September 2025, upholding the EU-US Data Privacy Framework adequacy decision.
- Court of Justice of the European Union, case register, Case C-703/25 P (Latombe v Commission appeal), filed 31 October 2025, pending..
- US Supreme Court, Trump v. Slaughter, decided 29 June 2026, 6-3, overturning Humphrey's Executor..
- noyb.eu, 'US Supreme Court just blew up EU-US Data Transfers', 29 June 2026 - Max Schrems quotation, verbatim.

Photo credits (Wikimedia Commons)

- European Parliament building, Brussels (hemicycle interior): Profpcde, CC0 - https://commons.wikimedia.org/wiki/File%3AEuropean_Parliament_Hemicycle_-_Brussels_2024.jpg
- Berlaymont building, European Commission headquarters, Brussels: almathias, CC0 - https://commons.wikimedia.org/wiki/File%3ABerlaymont_building_in_Brussels.jpg
- Court of Justice of the European Union towers, Luxembourg: Alf van Beem, CC0 - https://commons.wikimedia.org/wiki/File%3ATours_de_la_Cour_de_justice_de_l%27Union_europ%C3%A9enne_photo_2.jpg
- Googleplex, Google headquarters, Mountain View, California: Erik Möller, Public domain - https://commons.wikimedia.org/wiki/File%3AGoogleplex-SignIn.jpg
- Amazon Spheres, Amazon headquarters campus, Seattle: Andy Li, CC0 - https://commons.wikimedia.org/wiki/File%3AAmazon_Spheres_2018.jpg
- Meta Platforms headquarters, Menlo Park, California: LPS.1, CC0 - https://commons.wikimedia.org/wiki/File%3AMeta_Platforms_Headquarters_Menlo_Park_California.jpg
- Data centre exterior (generic, for GDPR/AI data-processing chapter): Rsparks3, CC0 - https://commons.wikimedia.org/wiki/File%3AData_center_roof.jpg

Not regulated financial advice.