
Da Ta
73
Pr otection
59
Broken
Badly

Today, our personal information is being collected, shared, stored and analysed everywhere. Whether you are browsing the internet, talking to a friend or making an online purchase, personal data collection is taking place. We are now at the start of the "internet of things", where more and more devices are connected to the internet, generating still more data.

In parallel, the age of big data is upon us. This means that, even when you are just sitting at home or driving your car, your TV, car or GPS system are generating and storing information. Public or private entities alike are interested in collecting this data, sometimes for innocuous reasons and sometimes for unpredictable ones. Following the Snowden revelations, we also know that intelligence services will do everything they can to get access to those data, including breaking security technologies.

One thing is clear, users must regain control over their personal data and companies and states must generate a culture of respect for citizens' data protection rights and privacy. These objectives are the prime motivations behind Commission's proposal for a Data Protection Reform package. The European Union is trying to establish a data protection framework that will put citizens' back in control of their personal data and ensure a high standard of protection for their fundamental rights to privacy and data protection. This reform would also bring harmonisation to the EU data protection framework and update the rules in place that dates back from 1995, where technology was very different from today.

Since 2012, the European Commission and the European Parliament both have produced a text that, while not being perfect, would greatly benefit citizens and businesses, establishing a common set of rules for the whole EU and guaranteeing high standards for personal data protection. Unfortunately, within the Council of the EU, Member State governments are working to undermine this reform process. For more than three years, the Council has not only failed to show support for this reform and negotiations, but is now proposing modifications to the text that would lower down the existing level of data protection in Europe guaranteed by the Directive 95/46 and even below the standards required to be in line with the EU treaties.

Four digital rights and privacy NGOs, EDRi, Access, Panoptykon Foundation, and Privacy International have produced an analysis of leaked and recent texts tabled by the Council through short one pagers highlighting the most problematic issues.

1 Data Protection Principles

WHY IS IT IMPORTANT?

The principles of data protection are the foundation on which the right to our personal data is built. If the principles are weak, then the entire structure will be weak and unreliable.

Under the existing legislation, companies can process data using one of six reasons. The first five can be summarised in two words – necessity or consent. The sixth one is more unclear – the "legitimate interest" of the organisation processing the data. In other words, they can decide that their interest in processing your data is greater than any possible harm to you from this processing. Currently, there are limitations on this – the purposes that your information is used for must be clearly defined (so called "purpose limitation"). This means, for example, if you give your data to a supermarket for your loyalty card, they can use this information for relevant and related purposes. They cannot sell your data to a health insurance company that will profile you as potentially unhealthy, for example, based on your food-buying habits. The individual should know 1. to whom she/he gave their data, 2. that only the necessary data can be collected and 3. that the purpose of collection must be respected. This gives predictability and control to the individual.

In short, data may only be processed when it is not excessive and is done for explicit and legitimate purposes.

HOW IS THIS BEING UNDERMINED?

The core of data protection is control and predictability. If you do not know who is using your information or what your data is being used for, then you clearly have no control.

WHAT IS PROPOSED?

Some of the Council's proposals gut data protection of all meaning. For example, the Council suggests that internet browser settings (failing to change the default to prevent tracking – or failing to change settings back, if a particular website requires you to change your settings) could constitute consent for being tracked and profiled online. Having removed the Commission's initial proposal for explicit consent and diluted the entire concept of consent of the individual, the Council then removes the final element of an individual's control of their data – the uses to which the data can be put, once they are collected ("purpose limitation").

The German position attacks this principle head-on. It proposed a demand forcing citizens to accept processing of their data for reasons of "overriding public interest," (recital 30) because individuals owe it to society to allow their data to be processed. However, they do specify that such processing must be "transparent". Transparency and purpose limitation is also undermined by Germany, which proposes that transfer of data to public authorities should be regarded as in their legitimate interest if the stated purpose is outside the scope of the EU legal framework. Germany undermines transparency still further by proposing that consent should cover unknown future uses of the data for "scientific" purposes.

As a final step to completely remove any link between the individual and their data, it has been proposed in the Council that data can be processed under the "legitimate interest" exception (consent is not needed if the company feels that they have a "legitimate interest" in processing data). This data could be passed on to third parties under the legitimate interest exception and those third parties could use the exception to start processing the data for reasons that are completely unrelated and incompatible with the original purpose. If a company you have never heard of can process your data for reasons you've never heard of, what is the point in having data protection legislation?

2 Data Subject Rights

WHY IS IT IMPORTANT?

In order to have a strong Data Protection framework, citizens or groups of citizens ("data subjects") need to have recognised rights that empower them to defend from attacks to their privacy and other fundamental rights. For example, if your name is in a debtor blacklist of a bank due to a debt you already paid, that could lead to not being able to receive a loan from any bank.

It is also important that governments don't have ways to produce profiles of citizens. Profiling is a process whereby assumptions are made about individuals based on automated processing of data which has been collected about them. This type of profiling is most commonly used for business purposes (for targeted advertising or credit rating, in particular) and for law enforcement purposes. Profiling tends to reinforce societal stereotypes and has a built-in acceptance of errors – the profile will guess who is a potential terrorist or a bad insurance risk.

HOW IS THIS BEING UNDERMINED?

Making it more difficult for people to be aware of what personal data is out there and when they get access to it means that they cannot change information that is false or outdated. This could lead to all sorts of consequences to the person, ranging from price discrimination to arrest orders.

Concerning profiling, strong safeguards should be put in place, including the right to be provided with meaningful information about the logic behind the profiling.

WHAT IS PROPOSED?

With regard to access to the information, the latest texts propose deleting the former Article 11 which had concrete obligations on how people, especially children, need to be informed in a "concise, transparent, clear and easily accessible policies" about how personal information is being used.

Also worrying is the re-insertion (after being deleted in the Parliament's approved text) of profiling as a possible exception to the rules that would be implemented in Member State law (Article 21). With this change, Governments can claim national security, defence, public security and even "other important objectives of general public interest" to profile citizens. This is basically providing a blank cheque to governments which, under various excuses, may start to profile people based on their online political activities and prepare, for example, blacklists who do not fit with the profile of "normal" citizens.

Price discrimination is another way in which profiling affects citizens. If companies can make profiles according to, for example, which websites you visit and how much are you likely to pay for a flight, you may face higher prices than another person checking the same flight at the same time. The fact that profiling might be wrong 5% or 10% of the time is not important from the perspective of the business targeting customers buying habits, but of potentially huge importance to the individual citizen. Research from the University of Cambridge shows that surprisingly extensive, sensitive and relatively accurate information can be obtained about an individual based on comparatively (in a world of "big data") small amounts of data.

3 Remedies, Liability and Sanctions

WHY IS IT IMPORTANT?

Good legislation is not effective without good enforcement, and good enforcement means citizens can have ready access to redress and justice, while the sanctions for the wrongdoers are effective, proportionate and dissuasive. One of the biggest failures of the current data protection legislation has been enforcement that varies widely across the EU; this has enabled larger companies to base their operations in countries with 'soft' data protection regimes, with little incentive to respect the law. It is shameful that, after 20 years of data protection legislation, access to justice is so ineffective that two thirds of citizens across the EU do not even know that a Data Protection Authority exists in their country.

It is crucial, to ensure the new Regulation has teeth, that authorities and courts have the power, when necessary, to impose an appropriate level of penalties. It is equally crucial that citizens have access to effective redress, and be compensated for the damage, material or moral, that they can suffer. For this to be feasible, associations defending citizen or consumer rights must also be able to lodge complaints or seek actions in court on behalf of groups of consumers.

HOW IS IT BEING UNDERMINED?

The nature of privacy infringements, whether data breaches or undercover online profiling, makes it all the more important to put actionable remedies in place –and the Council is working to stop this from happening.

If sanctions end up at a level that is not a real deterrent, it will continue to be cheaper for large enterprises to break the law and accept sanctions as an acceptable business expense.

WHAT IS PROPOSED?

Two key provisions are the right of public interest organisations to act on behalf of citizens and consumers by means of collective complaint actions (Art 73-76); and the level of penalties and sanctions that can be imposed on data controllers who flaunt the rules (Art 79).

Following the Council proposals, organisations can no longer be mandated by more than one citizen to complain on their behalf, therefore removing the possibility of class action suits. It is also unclear whether organisations could represent a group when taking action on their own initiative (collective action). Furthermore they are now restricted to taking such action only to Data Protection Authorities, not courts.

In the latter case, there is pressure to lower the amounts of administrative fines of up to 5% of yearly turnover for big enterprises, agreed by the Parliament.

4 “Risk-based approach”

WHY IS IT IMPORTANT?

Public and private entities collecting, processing and sharing your data are required to comply with a series of obligations under the Regulation. These obligations are a key element to ensuring that users have greater control over their personal data, as well as ensuring business best practices for secure and efficient data processing in the EU.

The increasing amount of high profile data breaches underlines the importance of making sure that companies notify customers of such breaches and work with data protections authorities. In addition to that, as we enter into the age of the “internet of everything” and the age of big data, companies should be adopting a proactive approach to privacy and security. This is laid down in the provision of data protection by design and by default. This approach is intended to rebuild citizens’ trust in products and services, to the benefit of the internet economy.

HOW IS IT BEING UNDERMINED?

The Council agreed in October 2014 on vaguely worded provisions on these matters and has opted to put the decision-making power into the hand of companies through a so-called “risk based approach”.

WHAT IS PROPOSED?

Under the Council approach, it will be up to the companies to decide whether or not to comply with obligations that would provide citizens with high standards of data protection and control over their own data. For instance, you would only be notified of a data breach if the companies determine under its own criteria that it represents a “high risk” for your fundamental rights.

The Council has undermined the essence of data protection by design and default by letting companies decide when and how privacy will be embedded into products and services.

These provisions agreed by the Council would undermine our privacy and would greatly reduce incentives for companies to improve data security.

5 “One stop shop” mechanism

WHY IS IT IMPORTANT?

The “one stop shop” mechanism is one of the primary objectives of the Data Protection Regulation. This approach aims at harmonising oversight and implementation of the Regulation, as well as guaranteeing effective remedies for users. At the same time, this mechanism would reduce the administrative burden on companies operating in Europe, providing legal certainty and predictability.

The “one stop shop” mechanism would simplify complaints, creating a single point of contact for citizens and business bringing a transnational complaint. It would also ensure consistent application of the Regulation through the European Data Protection Board, eliminating the current common practice of “forum shopping”.

HOW IS THIS BEING UNDERMINED?

This element has been one of the most politically charged in the reform proposal. In fact, the Council has been going back and forth on these provisions. All Member States originally agreed in October 2013 on a “one stop shop” mechanism. However, in December 2013, the Council went back on its decision and decided to reopen the negotiations.

In these leaked documents, the Council is proposing a highly bureaucratic and complex one stop shop mechanism which now resembles more of an “optional three stop shop”.

The then Fundamental Rights Commissioner Reding called out this political tactic: “We are effectively reopening questions which had been agreed in October. The questions we have been asked cast doubt on the fundamentals and call into question our central objectives. The One-Stop-Shop would become an empty shell. Bad for citizens and bad for business”.

WHAT IS PROPOSED?

Based on the leaked documents, the current proposed text from the Council on the “one stop shop” mechanism would add several levels of bureaucracy. In the case of a transnational complaint, at least two data protection authorities would have to be involved and reach consensus to solve the case. The European Data Protection Board would only be brought in case of conflict between the two or more data protection authorities involved in the resolution of the complaint.

Such a scenario could be very lengthy as data protection authorities would have to go back and forth before reaching consensus. It could also lead to a fragmented implementation of the Regulation as the oversight role of the Board would be greatly reduced. Both citizens and business would then be left without the benefits of a swift, predictable and harmonised “one stop shop” mechanism.


EDRi


access


PRIVACY
INTERNATIONAL


FUNDACJA
PANOPTYKON