

The EU's

Data Protection Reform

Published by **Jan Philipp Albrecht** MEP



GREEN EUROPEAN
FOUNDATION



The Greens | EFA
in the European Parliament

Imprint

Publisher **Jan Philipp Albrecht MEP**

European Parliament
Rue Wiertz 60
1047 Brussels
Belgium

Green European Foundation
15, Rue d’Arlon
1050 Brussels
Belgium
www.gef.eu

Editor **Ralf Bendrath**
Text **Jan Philipp Albrecht, Ralf Bendrath, Florian Jotzo, Zora Siebert**
Proof-reading **Levka Backen, Benjamin Breitegger, Pia Kohorst, Siana Rott**
Coordination of the English version **Fiona Costello**
Design and Illustration **p*zwe**
Print **AktivDruck, Göttingen**

December 2015

With the financial support of the European Parliament.



Table of contents

Foreword.....4

Why data protection? Where does the idea actually come from?.....6

The EU data protection reform: What is it about?.....8

Challenges in data protection.....10

Selling off our data.....12

The surveillance society.....14

Frequently asked questions

1. Who is the Data Protection Regulation really for?.....16

2. Will a law like this really work for the internet?.....18

3. Will the new data protection regime generate more bureaucracy?.....22

4. How can I assert my rights in the EU?.....24

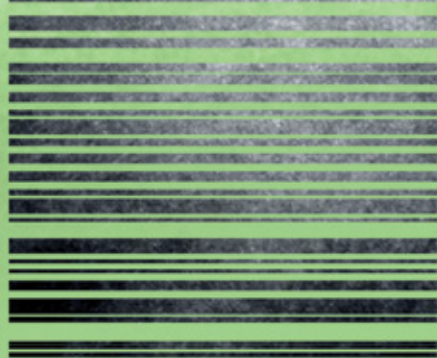
5. Does data protection wipe out the press, science and archives?.....26

6. What happens if data is transferred outside EU borders?.....28

How does EU legislation such as the Data Protection Regulation come into being?.....30

Lobbying and the Data Protection Regulation.....32

How can I protect my privacy on the internet?.....34



Dear reader,

Many people still see the words “data protection” and think they are something technical that does not really affect them. However, this is a mistaken notion. As well as being outdated, it is mistaken because data protection is in fact not about protecting data at all: it is about protecting people. When a census was planned in Germany in the early 1980’s, many people complained that the collection of their personal information (such as their income or religious affiliation) constituted a violation of their fundamental rights. The German Federal Constitutional Court ruled that a human right to “informational self-determination” arose out of human dignity and the right to free development of one’s personality. This cumbersome term marked the beginning of the long development of the fundamental right to data protection in Europe.

Nowadays it is not just every few years that how much we earn or what religious community we belong to is gauged. The digitisation and networking of all areas of life and all things means that, every second, we divulge a whole raft of information that can be – and, in the vast majority of cases, actually is – beamed around the world at almost the speed of light and stored in practically unlimited data centres until the end of time. The question then arises as to how we can remain in control of our lives and our own selves in this situation. Or have we already become products of a data-oriented society in which the large IT service providers have a firm grip on our work, economic activities and private life? This brochure aims to provide answers and background both to these questions and to the potential political and personal action that can be taken.

With best data protecting regards,

Jan Philipp Albrecht

Member of the European Parliament, Vice-Chairman of the Committee on Civil Liberties, Justice and Home Affairs, Rapporteur for the EU Data Protection Regulation



WHY DATA PROTECTION?

Where does the idea actually come from?

The saying “my home is my castle” was coined as long ago as 1604, in England. The notion arose in the context of a legal dispute and limited the right of the king’s soldiers to enter a house unannounced and without a reason. The right to privacy therefore initially extended to one’s own four walls. An additional concern for “informational self-determination” arose starting in the late nineteenth century. In 1895, Boston lawyers Samuel Warren and Louis Brandeis wrote an essay entitled “The Right to Privacy”, in which they laid out the right to control what other people know about us. The impetus for this essay was provided by technological developments that were new at the time: the first hand-held cameras for taking snapshots and the emergence of modern daily newspapers had given rise to the

first paparazzi, whom Warren and Brandeis wished to counteract. Even then, the aim was not to resist technology or innovation, but rather to foster the dignified use of these things so as to respect people’s right to self-determination.

Automated machine processing of data was developed in the 20th century. Even prior to the invention of the computer, punch cards were used to process large quantities of data automatically. This played a role in technical calculations, but punch cards also enabled information about people to be automatically processed – for administrative purposes, for example. The Nazis, too, used punch card machines from IBM subsidiary Hollerith to organise the industrial mass murder of Europe’s Jews.

When authorities and businesses started to use mainframe computers in the 1960s, a broad debate took place about the power of these new machines. Then, as now, the idea of data protection was to make the most of the opportunities and possibilities offered by new technology without reducing people to mere objects of automatic computer operations. It was then that the concept of “data protection” was developed.

Data protection is, at its core, not a technical matter. It is not data that is to be protected, but people. Data protection is about our ability, in this digitised world, to make our own decisions regarding who can know something about us, what is done with this data and the possible effects on our lives. The German federal state of Hessen brought in the world’s first data protection law in 1970. Discussions also took place in the United States during the student protests about whether computers should be used for the purposes of political control – by means of databases of radical opposition figures, for example. In response, the US Privacy Act was adopted in 1974. However, this act only regulates data protection with regard to the authorities; there is still no comprehensive American law on data protection with regard to companies.

National data protection legislation gradually appeared, primarily in the European Union. These laws set limits on data processors and granted rights to those affected – i.e. us – to receive information about data or to delete it, to take two examples. In its landmark decision on the 1983 census, the German Federal Constitutional Court coined the more accurate term “informational self-determination”. As an increasing amount of information on our lives is available digitally, we must have the right to determine

who knows what about us and what they might be able to do with that information with the help of a computer. The Federal Constitutional Court very perceptively recognised that a society in which we feel constantly observed, recorded, evaluated and scanned is no longer an open society of free and equal people.

In 1980, Council of Europe Convention No 108 and the Organisation for Economic Cooperation and Development (OECD) guidelines made a first attempt to harmonise the right to data protection at international level and thereby to take account of the increasingly international circulation of data. The hitherto most decisive step taken by the European Union is Directive 1995/46 on the protection of personal data, adopted in 1995. The EU Charter of Fundamental Rights – which has been binding on the European legislature since 2009 – stipulated that data protection was a fundamental right in the EU as well.

Unfortunately, many companies do not comply with European data protection law and do what they want with our data. Thus the present EU data protection reform is the next major step and it aims to guarantee that we can finally exercise our rights effectively. The EU’s data protection reform is an attempt to reclaim our digital self-determination. It is also a component of the completion of the European digital single market.



The EU data protection reform: WHAT IS IT ABOUT?

The principles of European data protection are still sound. Unfortunately, enforcement in several EU Member States is very poor: data protection authorities are poorly equipped and the fines that they can administer for violations amount to small change for many large companies. At the same time, law-abiding companies that want to respect our data protection have to contend with 28 different laws if they want to operate across Europe and make use of the single market. The many companies that have only one European office and use the internet to offer their services to the entire single market also pose a major problem for customers, who have the labori-

ous task of grappling with the legal system that applies at the company's headquarters if they wish to raise an objection and exercise their rights. The Austrian student Max Schrems is an example of this: he had to bring a court case in Dublin, at great expense, in order to assert his claims against Facebook.

Meanwhile, firms that offer online services here from outside the EU often show complete disregard for European law. If the American IT industry in Silicon Valley, and elsewhere, does not respect the rules in the same way as European companies, then poor enforcement of the law means that its location

gives it a clear advantage. Moreover, both American and European companies often conceal information about what actually happens to our data within data protection statements that are long and difficult to read.

The EU has therefore been working for several years on a new data protection law. Numerous public consultations took place starting in 2009, and the Commission issued a communication on “[a comprehensive approach on personal data protection in the European Union](#)” in November 2010. The European Parliament and the Council of the Home Affairs and Justice Ministers of the EU Member States responded with their own opinions in 2011. As early as this stage, the European Parliament made it clear, among other things, that a reform must under no circumstances lower the existing level of data protection.

In January 2012, the then EU Justice Commissioner Viviane Reding presented the long-awaited draft law. Since then, the European Parliament and the council of Member States (the Council of Ministers) have been working to arrive at a version of the law that both would find acceptable. In the European Parliament, the efforts are being led by Jan Philipp Albrecht, a data protection expert from the Greens. The presidency of the Council rotates between the Member States every six months.

The data protection reform has three goals: to strengthen our rights and better enforce them; to make it easier for businesses to comply with European rules; and to make computer systems that promote data protection the norm.

1) High fines are planned in order to ensure that our rights are better enforced, as are consumer protection instruments, such as group litigation or class actions (the ability for associations representing data protection, consumer protection or other public-interest causes to initiate court proceedings). Meanwhile, coupling is prohibited (i.e. the provision of a service cannot be made conditional upon the collection of more data than is necessary). Those affected are to have the right to consult their data in electronic form and to reuse this data for other services. Standardised symbols are to provide at-a-glance information about what is happening with data, like organic food labels.

2) In order to make matters easier for businesses, an EU regulation will replace the previous directive with immediate effect. This will establish a uniform law across the whole European Union, replacing the current patchwork of 28 different national laws in the Member States. In addition, bureaucratic requirements are to be simplified or scrapped.

3) Technological data protection should better ensure in future that less data is produced in the first place, that only data that is strictly necessary for the provision of a service is stored, and that services can be used anonymously or pseudonymously. There are also new rules governing design that promotes data protection (“[privacy by design](#)”) and default settings that involve less data (“[privacy by default](#)”). The right to take our data in machine-readable form to other providers will facilitate competition.



CHALLENGES in data protection

An increasing amount of data on each and every one of us is being collected and processed:

German consumers now take one hundred million loyalty cards such as Payback or Happy Digits with them when they go shopping, providing businesses with a detailed insight into people's everyday consumption habits.

The social network Facebook uses social plugins such as the “like” button to monitor internet users' movements, even on external websites outside its own infrastructure. The “friend finder” function provides the American business with a broad overview of internet users' social environment. Thus even people who are not signed up to Facebook end up in this U.S. company's data stores. As well as Facebook, the operators of Facebook fan pages can view this data and share it with advertising firms.

Smartphone and tablet apps, too, which are so useful in daily life, like to find their way into their users' address books, calendars and location data, which are saved on devices. Even apparently innocuous and free applications such as the torch tool “Flashlight” seize calendar and GPS data stored on devices, data that is wholly unrelated to their function. The increasingly popular health apps are another example. They gather information about our heartrate, blood pressure, blood oxygen level, blood sugar level, sleep patterns and bodyweight – and then sell this information on for marketing purposes.

By employing big data techniques, companies are able to analyse and make use of unprecedented quantities of information. The case of the Uber smartphone app demonstrates what intimate details companies try to extract from these mountains of data. The provider of this app analysed its customers' movement data in order to predict whether they were using the service to get to one-night stands. Aside from such extreme examples, companies' use of data is mostly mutually beneficial: delivering targeted advertising and improving their products. More comprehensive information, however, can also enable them to reduce typical risks related to their business model, at the expense of customers. For example, decisions relating to payment by instalment. People who the statistics say are more likely to fall behind on repayments pay a higher interest rate, even if they might be very reliable in individual cases. Companies' options in this regard will continue to expand rapidly over the next few years. The “cloud”, the “internet of things” and “wearables”, with smart watches, televisions, heating controls, refrigerators and cars, will all enable data-hungry computer systems to burrow even deeper into our everyday lives than we are used to with today's computers and smartphones. This means that much more accurate profiles of us will be put together. It is one of the great challenges of our time to ensure that every person in this digital environment can in future be aware of who knows what about them. The data protection reform aims to bring this about.

SELLING OFF OUR DATA

Footprints in the snow fade away. Digital ones do not. Google and Facebook monitor even users of other websites for months at a time. Thus, they track people's internet behaviour, regardless of whether these people are registered users of these two US providers. Traditional information processors such as the Bertelsmann subsidiary Arvato Infoscore collaborate with digital information gatherers and the American market leader Acxiom now has files on around 700 million people containing up to 3,000 individual pieces of information per person. The stored data includes information on their education, housing situation, employment, finances, interests and health. Acxiom already has 44 million Germans – more than half of the population – in its holdings. Digital interfaces are also growing rapidly in everyday life. Germans possess over 100 million loyalty cards, and these combined with payment information from

debit and credit cards provide companies with a detailed picture of consumers' purchasing and payment habits.

These data trails make us predictable: insurers and banks are able to use data analysis to reduce the typical risks related to their business model at the expense of customers. For example, the Hamburg-based ratings company Kreditech uses location data and social media profiles on Facebook, Xing and LinkedIn to provide credit ratings. Life insurance company Aviva is investigating models that use consumer behaviour, lifestyle and income to predict who will develop diabetes, high blood pressure or depression and who therefore must pay higher premiums. The insurance company Generali wants to encourage its health insurance customers to gather information on their nutrition, fitness, healthcare and lifestyle via

smartphone. The reward consists of vouchers or discounted premiums. People who do not comply could pay higher premiums in future. Allianz has similar plans. This company is working together with car manufacturers to create rewards programmes for its car insurance policies involving in-car GPS systems that automatically record individuals' driving behaviour. Meanwhile, companies can use consumer data to draw conclusions about their customers' personal circumstances. The American supermarket chain Target, for example, uses this data to ascertain whether its customers are likely to be pregnant. The company targets expectant parents particularly around the suspected due date, as their consumption changes enormously at this point and they are especially susceptible to advertising. Sellers also use data analysis to deliberately disadvantage consumers when setting their prices. The travel site Orbitz, for example, used

browser information to ask up to 13% more from Apple users for the same hotel room because they were categorised as having more money to spend.

In this context, anyone can become a victim of statistics. Ratings agencies make mistakes when gathering and interpreting data, and statistical probability is not equivalent to individual people who are affected. The developments that have been detailed here primarily discriminate against people who do not fit into the statistical framework. The same is true of people who wish to avoid being monitored. Increasingly, they have to make do with higher prices, as even a lack of information about them represents a risk for companies, to which their reaction is to raise prices. This puts more pressure on consumers to disclose more information. Thus the right to data protection is becoming an expensive privilege.



THE SURVEILLANCE SOCIETY

The unprecedented revelations made by Edward Snowden show to what extent US and UK intelligence agencies, together with their counterparts from Canada, New Zealand and Australia, are secretly monitoring people around the world. By means of Prism, US authorities make massive use of data from the data centres of major American IT service providers such as Microsoft, Google, Yahoo and Amazon. GCHQ, the British secret monitoring service, uses Tempora to tap into key transatlantic data flows, seizing a large proportion of international data transfers and analysing this information. GCHQ has also systematically gained access to emails belonging to journalists working for international media organisations. It has also infiltrated the infrastructure belonging to the Belgian telecommunications firm Belgacom, used by members of the European Parliament and other EU institutions. Like GCHQ, the NSA – the American monitoring agency – has also targeted governments: even allies such as the German chancellor Angela Merkel, whose mobile phone was breached, figure among the 122 heads of state worldwide who were bugged. Although the EU data protection reform does not concern itself with Snowden's revelations, they nonetheless strongly influence the law. They caused political debate to focus on the issue of the surveillance society – and hence on data protection.

But unchecked mass surveillance by intelligence agencies does more than jeopardise citizens' fundamental rights: it threatens companies in equal measure, as they mostly use hardware and software from American suppliers. These suppliers more or less willingly allow their domestic intelligence services to have broad access to even the most sensitive data.

Given the threats posed by terrorism and international organised crime, the calls at European and national level for more state surveillance are becoming louder: car registration number recognition, the "Bundestrojaner" ("state trojan") spyware, the SWIFT agreement to exchange international banking data and, first and foremost, the collection of information on airline passengers and the retention of data. These are just some of the prominent topics currently being debated. The judgements of the European Court of Justice and of the German Federal Constitutional Court on the subject of data retention show that legislatures have been too hasty to jeopardise people's fundamental rights and freedoms out of a desire for more security. In both landmark judgments the courts showed that groundless retention of data is incompatible with both European and German fundamental rights.

It is therefore incumbent on lawmakers to come up with less simplistic responses to the challenges of counter-terrorism and modern policing, responses that do not view collective security and individual freedom as contradictory. In addition, the state must effectively protect its citizens from surveillance by intelligence services.



FREQUENTLY ASKED QUESTIONS

1. Who is the Data Protection Regulation really for?

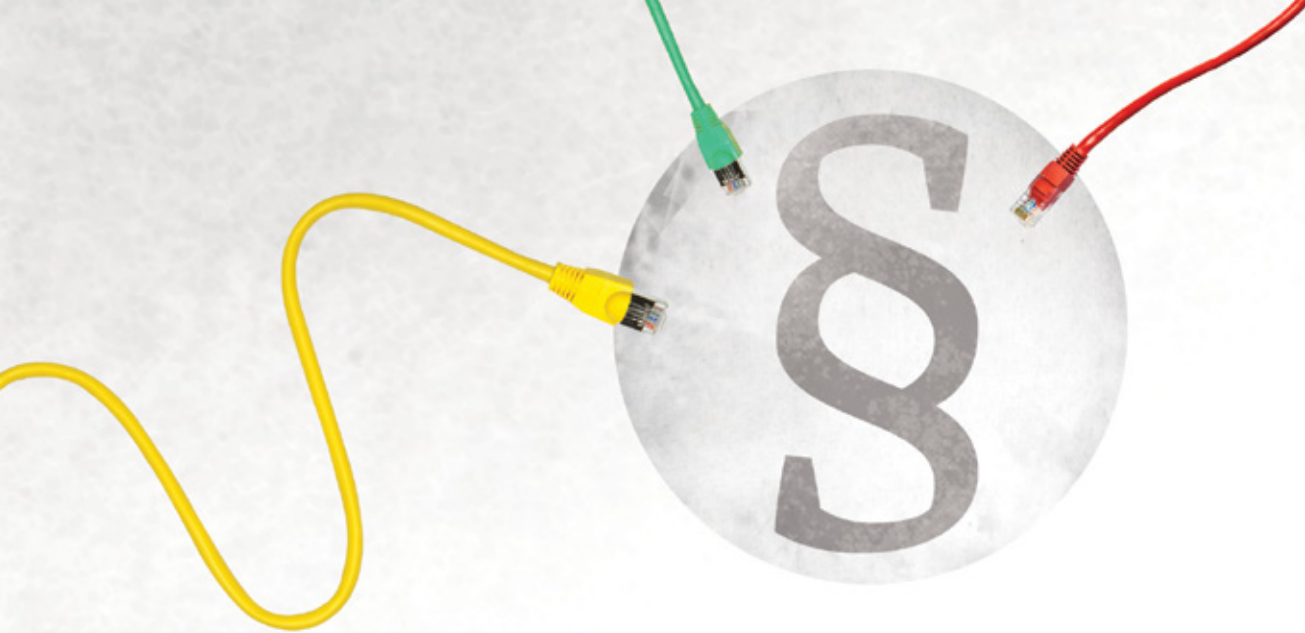
At the outset of the EU data reform, the question was “why” – why does the current framework set out in the EU Directive of 1995 need reforming and, moreover, why do steps need to be taken towards a unified European data protection law, the EU Data Protection Regulation? The answer is very easy: because data, unlike the traditional circulation of goods, crosses borders in milliseconds and it is becoming increasingly difficult to tell where exactly our data is saved. Companies whose business is data therefore find it very easy to say that, “Your German data protection laws have absolutely no bearing on us because we process your data in Ireland or in the US.” There is a paradox here, especially with regard to the European Union: companies based in one EU Member State can offer their services via the internet throughout the entire single market. If they do not respect the laws of other EU Member States, these other countries’ authorities cannot force them to comply; only the authorities in the place where the company is based can do that. A common set of rules for the entire EU market is therefore required. The idea is an EU regulation that stipulates, following the principle of *lex loci solutionis*, that all companies in the world must comply with the uniform rules set out in this regulation when they offer their goods and services on the European market. If they do not comply then they are liable for penalties that are uniformly high across the whole of Europe and can be enforced worldwide. However, this approach is only possible if all 28 EU countries agree on a unified and legally robust data protection standard. The European Parliament has already done so; an agreement with the Council of Ministers still remains to be achieved.

Of course, it must be borne in mind when carrying out such a harmonisation that there are specific areas where Member States’ rules and legal cultures still vary considerably. As early as its proposal of January 2012, the European Commission had stipulated that specific, national rules could be enacted regarding media freedom, research, churches, professional secrecy and workers’ rights. The European Parliament extended this into additional areas such as public social insurance schemes and archives. There is another important and frequently misunderstood part of the reform. The new data protection regulation does indeed also apply to the way authorities process data, so that, for example, people can ensure that the authorities respect their requests for disclosure and erasure. However, the regulation explicitly stipulates that processing of data by authorities must always (!) be subject to a national law that clearly de-

All companies in the world must comply with the uniform rules set out in this regulation when they offer their goods and services on the European market.

scribes the scope and conditions of the collection and processing of the data. The regulation therefore will not restrict – and will by no means supersede – government authorities’ legal rules

relating to data protection. In its position, the European Parliament once again made national legislatures’ room for manoeuvre very clear.



2. Will a law like this really work for the internet?

Law for the digital single market, not specific regulation of technology: it has been argued many times that the current EU Data Protection Directive from 1995 must be replaced because it was promulgated before the internet became widely used. That is correct. The Data Protection Regulation is primarily intended to establish a unified regulatory framework for the digital single market that has come into being. It also aims to ensure that the law is enforced against companies that offer services on the European market from outside this market – namely, over the internet. However, it by no means intends to regulate specific technologies such as the internet or online services or protocols. A law aiming to do that would very quickly become obsolete. It would scarcely be possible for lawmakers to decide new

rules for all new technological developments such as smart electricity grids, the internet of things or networked cars.

Fundamental principles of established data protection law: fundamental principles will not be altered: collection and processing of personal data only when those affected give voluntary consent or when at least they can assume – on the basis of data protection declarations, legal regulations or an existing relationship to the data processor – that this will happen; the right to disclosure, correction and erasure; the requirement that data be collected for a specific purpose; data minimisation. Specific application to individual technologies and business models is left to national data protection authorities. Unfor-

tunately, the European Parliament and the Council of Ministers take significantly different positions regarding even these basic principles. As an example, the European Parliament restricted the “**legitimate interests**” of the data processor – which allow data to be processed without the consent of the person concerned – to what can be reasonably expected. Thus any existing customer of a company can expect to periodically receive current offers, provided these have not been refused. However, it is not to be expected that this company would sell data to completely unconnected businesses. On the other hand, the Member States are discussing whether it should be permissible for data to be processed for entirely separate purposes – even by unknown third parties – than those for which the data was collected. This, however, would reduce people’s rights to a level far below that proposed by the Commission, and below even the current level of data protection.

Definitions that will stand the test of time: Any information that can be directly or indirectly attributed to an individual is protected as personal data. This is important, particularly in an era of big data, when more and more data can be brought together, combined and analysed. There should therefore be incentives to use pseudonymised data, which cannot be linked to other data relating to the same person. The European Parliament has also clearly stated that data does not necessarily have to enable the (even indirect) identification of an individual’s identity in order to count as protected; it is enough that a person can be identified as being among a large number of other people. This is not intended to counter big data: many new applications that process large amounts of data do not require personal data. Anonymised data can be used that no longer allows in-

dividuals to be identified. Such applications are not restricted by the data protection law.

Informed consent as a cornerstone: Users must be informed about what is happening with their data and must in principle agree to – or refuse – their data being processed. While the European Parliament is insisting on “**explicit consent**”, as proposed by the European Commission, the Council of Ministers wants the much vaguer term of “**clear**”. This would give the data processors a way to avoid having to get consent as they could declare that the use of an online service comprises “**clear**” consent to data processing. Facebook has done this repeatedly: simply having signed up to the website is interpreted as giving consent to terms and conditions that have since changed. Moreover, the European Parliament wants to add easily recognisable symbols to lengthy terms and conditions and privacy statements so that users can assess the essential aspects of data processing at a glance. For online services, these symbols should be machine-readable and could therefore be identified by browser plugins, for example. Thus computers, making use of users’ settings, can automatically decide which websites are trustworthy and which are not.

Few, but important, technical rules: The regulation will also include technical rules in several places. But they are framed broadly enough to be generally applicable. They include the possibility of pan-European certification of data protection compliant technical standards such as Do Not Track or restricting automatic profiling, i.e. the electronic assessment of behaviour by which a computer determines an individual’s opportunities for social participation. When requested, providers will also be able to hand over

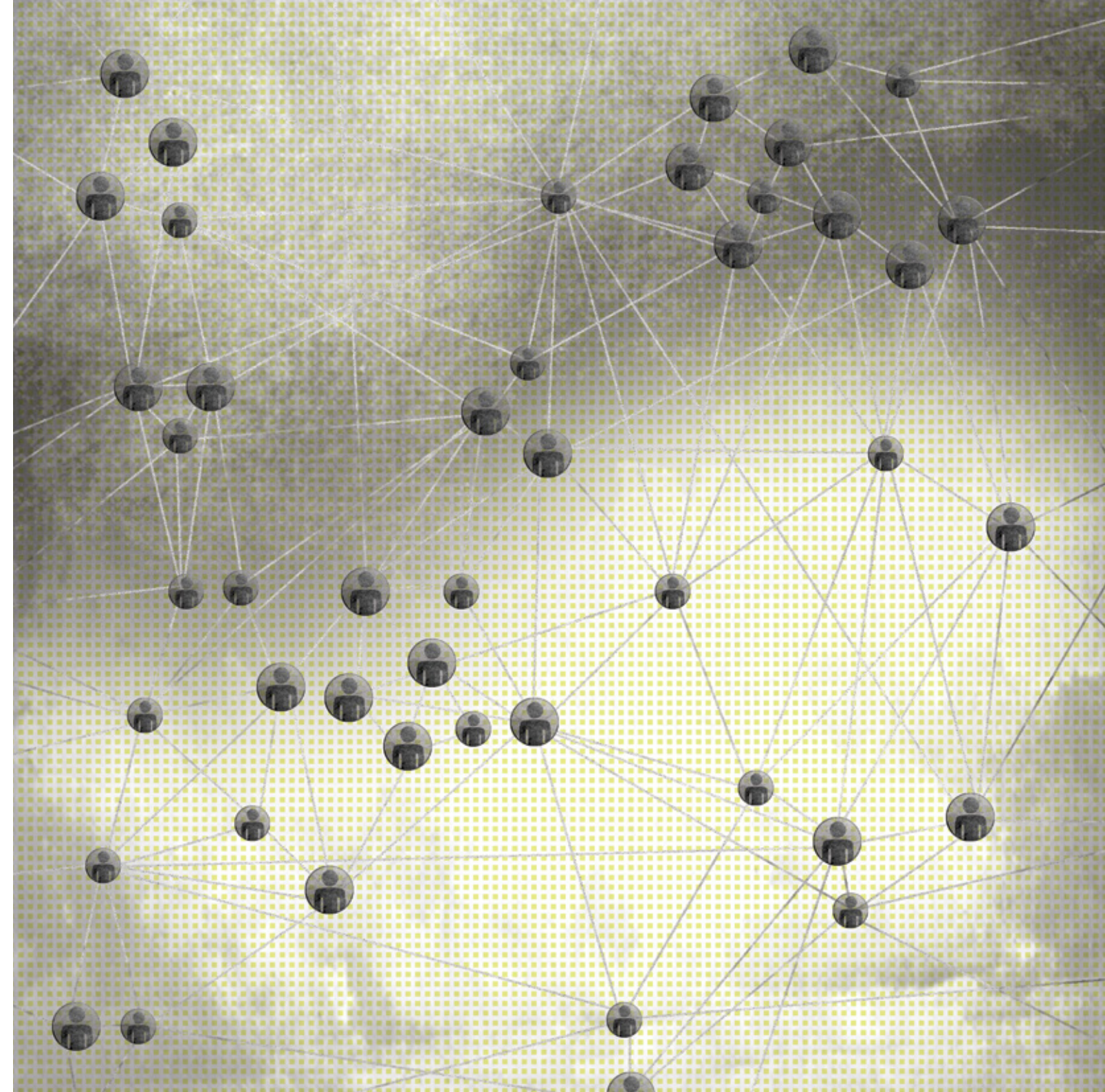
user data quickly, free of charge and in a digital, reusable standardised format, or transfer it directly to another platform. It is no longer logical in the 21st century for data to be provided on paper or in virtually useless PDF format.

Privacy by Design and Privacy by Default: Data processors and IT system developers must design their systems in a way which minimises the amount of data required and provides privacy by default settings. A strict principle of purpose limitation applies. This means that only data genuinely required to provide the service is collected. A smartphone app featuring only a torch function will therefore no longer be able to forward my address book to the firm providing the app. The European Parliament has expressly provided for a ban on coupling. This is intended to prevent services being used for excessive data collection on the basis of a single request for consent. Furthermore, it must be possible to use services anonymously or pseudonymously.

Right to be forgotten: Anyone wishing to have their personal data erased must be able to exercise the long-standing “right to erasure” against data processors. The latter must pass on the request for erasure to any third parties to which they have disclosed the data. The controversial “right to be forgotten” has been restricted by the European Parliament: only those who have published data illegally must also ensure that every copy is deleted. While the European Parliament considers the “right to be delisted” invoked in the European Court of Justice’s Google Spain judgment to be already covered by the legislation, the Member States are still discussing whether additional clauses relating specifically to this area

are required. However, the options open to the European legislature are limited as the EU cannot pass laws on freedom of expression or freedom of information. This can only be done by the Member States. The regulation requires Member States to balance freedom of expression and freedom of information against the protection of personal data. It is important that this balancing of fundamental rights is not carried out in the final instance by a private firm such as Google with a self-appointed advisory body. This must remain the task of data protection authorities and the courts.

Self-determination and regulation of internet traffic: It is often cited as an argument against data protection that many young people wish to put everything about themselves online. Nobody wishes to prohibit anyone from doing this. However, those who do not wish to disclose everything about themselves must also have the right and opportunity not to do so. Similarly, anyone wishing to disclose a lot of information about themselves must be able to expect internet services or data handlers to comply with fair rules.



3. Will the new data protection regime generate more bureaucracy?



Time and time again it is claimed that the Data Protection Regulation will lead to an increase in bureaucracy for businesses. The opposite is true: the new EU regulation would mean the 28 different Member State laws would be replaced by one pan-EU regulation. Given that the vast majority of companies already offer their products in more than one EU country, a unified regulation would actually lead to less bureaucracy for all. Furthermore, in its resolution on data protection reform the European Parliament reduced the bureaucratic obligations for data processors to the absolute minimum required to safeguard the rights of data subjects and introduced numerous facilitation provisions for small and medium-sized enterprises. It is clear therefore that the Data Protection Regulation will not create additional burdens for most businesses. Only in cases where extensive data processing takes place or, for instance, where sensitive data is processed does the European Parliament require, for example, that the business must appoint a data protection supervisor. This does not have to mean creating a new specific position. Depending on the scale of data processing carried out in the business, existing employees can be made available for only a few working hours, or the task can be undertaken by external data protection officers. In Germany, unlike in many other EU Member States, this is already common practice. For German companies in particular, the regulation would therefore ease a significant burden it faces when competing with other companies in the EU market.

In any case, the regulation provides huge opportunities for EU companies which outweigh any costs associated with adaptation. Treating all compa-

nies equally under one single data protection legal framework would eliminate the disadvantage in international competition which has existed for years. This means companies in Germany and other EU

For German companies in particular, the regulation would therefore ease a significant burden it faces when competing with other companies in the EU market.

Member States cannot simply take advantage of being well established and usually medium sized to switch to another EU country and so exploit the supposed

advantages of “weaker” data protection regulation. Large internet companies from Silicon Valley, such as Google, Facebook or Amazon, on the other hand, enjoy a relatively free choice of where to establish themselves in the EU. They have huge leverage when choosing their place of establishment, which they can use to increase pressure on host countries to adopt a softer approach to data protection controls or corporation tax. All that is usually required for these companies to be established is a post-box and a reasonable internet connection, to in turn determine data protection standards for more than 500 million Europeans. This situation constitutes a hidden subsidy for the major US internet companies. The EU Data Protection Regulation would be the most significant step towards providing adequate support for Europe’s IT economy.



4. How can I assert my rights in the EU?

One fixed contact point for Europe as a whole: The one-stop shop approach means that individuals right across the EU only need to contact the data protection authority in one country. The parties concerned can lodge their complaint with the data protection authority in their own Member State, irrespective of where the data breach took place. Similarly, companies only have to cooperate with the data protection authority of the Member State in which their head office is located.

Class action (group litigation): As is the case for consumer protection law, associations which support data protection, consumer protection or similar non-commercial interests are to have recourse to legal action.

Consistent law enforcement: A European Data Protection Board consisting of national supervisory authorities will ensure that data protection law is applied consistently and, in cases with Europe-wide significance, will make binding decisions – similarly to the case with competition law and banking supervision. In future, a race to the bottom will therefore no longer be possible in Member States with weak

enforcement. The European Parliament and the Council of Ministers have agreed on this approach in principle and do not wish the European Commission to have the final say – this will protect the autonomy of data protection authorities. A common regime also means that data protection authorities will require more resources and more staff.

Effective sanctions: Infringements are not trivial offences and sanctions are intended to hurt. To date this option has been largely lacking for data protection authorities in Europe. The Commission had proposed fines of up to 2% percent of annual global turnover for severe cases and the Member States appear to wish to stick to this. The European Parliament wishes to increase this to up to 5% of annual turnover or EUR 100 million. This will ensure that companies do not simply price in the cost of data protection violations. Fines must of course always be proportionate. Small undertakings should therefore not fear being made bankrupt due to minor infringements.



5. Does data protection wipe out the press, science and archives?

Data protection is a fundamental right and is enshrined as such in the EU Charter. However, like all fundamental rights, it is not an absolute or “super” fundamental right. Freedom of expression, freedom of research, freedom of the press and other fundamental rights should also be taken seriously and protected. In cases where these conflict with one another, the legislature and, as a last resort, the courts, are called upon to strike an appropriate and fair balance.


In the case of freedom of the press, it is clear that public figures can be reported on, even against their will. EU Member States already have regulation that makes this kind of distinction. Germany, for example, distinguishes between an “absolute” and a “relative” public figure: in cases of doubt an absolute public figure such as the chancellor must accept that her private life be reported on and that this information be somehow systematised and stored where it can be easily retrieved. Under data protection law she would have no right to erasure. A relative public figure, on the other hand, may only be reported on in connection with an event relevant to the press (such as local elections). All of this is already regulated by press and privacy law in the EU Member States and will not be altered by the data protection reform. This would in any case not be possible as the EU has no legislative competence in this area. For this reason the Data Protection Regulation expressly stipulates that Member States must strike a reasonable balance between the protection of privacy and the right to freedom of the press and freedom of expression.

Anyone wishing to use personal data for research must as a rule request permission from those concerned. This is required not only under data protection but also by the ethical principles of almost all academic associations. The European Commission had provided for broad exceptions, which would ultimately have even allowed the publication of medical data – i.e. particularly sensitive data – for research purposes. The European Parliament strengthened protection for those concerned and removed these aberrations. At the same time, it clarified that where

research serves a significant public interest, personal data, including medical data, may be processed without the consent of data subjects. This ensures that disease control or cancer registries, for example, remain unaffected. Additionally, the European Parliament introduced the possibility of giving consent to data processing for future, as yet unplanned research projects. Here again EU Member States can opt to regulate the details more precisely in national law as there may, for example, be different social and historical understandings of what constitutes a “significant public interest”.

Historical and scientific archives are also partially exempt from data protection. In the future, it will not be possible to rely on the right to erasure of personal information to rewrite history and falsify historical archives. Again, EU Member States can regulate the details themselves. Archives were already exempt from these rules regarding historical research in the Commission’s draft. However, because of frequent misunderstandings, the European Parliament has introduced a separate article on archives for clarification.

The important thing is that all of this applies solely to personal data. Research with – and the archiving of – anonymised data that can no longer be linked to the individuals concerned are not covered by the data protection law and will not be subject to any restrictions.



6. What happens if data is transferred outside EU borders?

There has been a great concern among the public about where their personal data end up, particularly since the revelations of Edward Snowden. The new EU Data Protection Regulation can go some way towards restoring our data sovereignty. It does not regulate what criminal prosecutors or secret services are permitted to do with our data. For the former, a separate EU directive is being negotiated simultaneously. In the case of the latter, the EU does not have authority to pass laws. The Data Protection Regulation does, however, regulate data collection

by businesses – and where less data is obtained, less can be tapped by intelligence services. The transfer of personal data to countries outside the EU is also regulated.

The European Parliament insists that European companies should not be permitted to pass on data directly to authorities in countries outside the EU. This is only to be permitted in accordance with European law and any legal assistance agreements based on it. This protection against foreign access to European data was already included in the initial Commission proposal but was deleted following intense lobbying by the United States government. The European Parliament has reintroduced it following the Snowden revelations. Whilst this approach is not included in the Member States' text, they seem to be in favour of it. In the meantime, with the LEADS Act (Law Enforcement Access to Data Stored Abroad), the US Congress has tabled a bill which would respect the EU rules.

Personal data may in principle only be transferred to countries outside the European Union for further processing if there is a suitable level of data protection in place, for example, under separate data protection legislation. Deciding which countries meet the European standard has so far been the preserve of the European Commission. The European Parliament wishes to obtain a right to veto this far-reaching decision, as it has for most other agreements with third countries.

Since the USA has no comprehensive data protection law and therefore cannot offer a suitable level of data protection, the European Commission and

the US Department of Commerce resorted in 2000 to a ploy. US companies can certify themselves as compliant with data protection and then qualify as “safe harbors” where the processing of European data is also permitted. Even at the time the European Parliament found this solution to be inadequate and has since then consistently rejected it. Aside from the fundamental issue, the “safe harbor” principle constitutes a de facto competitive advantage for US firms as they must comply with considerably fewer requirements than businesses based in the EU.

The European Parliament does not wish to allow contracted data processors to move our data back and forth across the globe. If this were permitted, neither data subjects nor data controllers would have the slightest idea of where in the world the data are being processed.

The EU and the USA have come into conflict during the negotiations on the TTIP (Transatlantic Trade and Investment Partnership) and the TiSA (Trade in Services Agreement) international free trade agreements. Whilst the European Commission has a clear negotiating mandate to keep European data protection out of these negotiations, US negotiators want to prohibit restriction of the free flow of data (including personal data). This would mean that the EU's attempt, for example, to protect itself against mass surveillance by the US secret service organisation, the NSA, by terminating “safe harbors” would constitute a barrier to trade and therefore be prohibited. It must be made clear that data protection is a fundamental right and is non-negotiable.

How does EU legislation such as the **DATA PROTECTION REGULATION** come into being?

A lot of discussion, drafting and formulating takes place in the EU before a law comes into force. The process involves countless stakeholders.

In the so-called ordinary legislative procedure, which is the EU's main legislative procedure, the European Commission has the sole right of initiative and therefore only it alone can put forward a legislative proposal. This proposal is the result of a comprehensive consultation process. This means that associations and interested parties are invited to express their stance and views on the preparatory work being carried out by the Commission. In the case of the Data Protection Regulation, the European Commission collected opinions and standpoints for eighteen months and its legislative proposal was issued in January 2012.

Once the Commission's proposal is presented, it is sent to the Council of Ministers and the European Parliament. The European Parliament appoints a committee and a "**rapporteur**" to examine it. This committee then discusses amendments to the Com-

mission document. The committee responsible for the Data Protection Regulation is the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) and the rapporteur is Jan Philipp Albrecht of the Greens. As rapporteur, he was heavily involved with the Commission proposal and presented his report – his proposals for amendments to the draft legislation – in January 2013. Also involved alongside Jan Philipp Albrecht are the "**shadow rapporteurs**": MEPs from the other political groups responsible for the process. Amendments can be tabled by any member of the European Parliament at the committee stage. The committee then reaches an agreement on the report and any amendments. In October 2013, the members of the LIBE committee agreed on a compromise text based on 4000 amendments! MEPs are popular targets for lobbying. The intensity of the work done by lobby groups and associations regarding the Data Protection Regulation is well reflected in the fact that amendments were often taken verbatim from the comments submitted by companies (see www.lobbyplag.eu).



Following the vote in the committee, the plenary votes on the proposal in what is known as the first reading, which often mirrors the vote of the committee. This was the case for the Data Protection Regulation: in March 2014, the plenary almost unanimously adopted the text negotiated by Jan Philipp Albrecht as the position of the European Parliament. The Parliament's position was then forwarded to the Council of Ministers. It, too, sets out its position on the Commission proposal.

The work in the Council runs in parallel to that of the Parliament. The Council of Ministers has been experiencing difficulties regarding the Data Protection Regulation. After the Parliament adopted its compromise in March 2014, the Council came under pressure and only then did it start to gradually reach an agreement. As with the Parliament, there is no time limit for reaching an agreement at the first reading.

The Council's position is crafted by the embassies of the Member States in Brussels and their experts

from their capitals. These embassies and Member State governments are also targets of lobbying.

Once the European Parliament and the Council of Ministers have adopted their respective positions, they enter into three-way negotiations with the European Commission – what is known as the "**trilogue**". Trilogues are intended to strike a balance between the interests of the three institutions. This usually requires numerous meetings, compromises and concessions. Generally, the European Commission acts as an intermediary between the Parliament and the Council in these negotiations. However, as a last resort, it may also withdraw its proposal or submit an amended version of the draft law.

The process is complete once an agreement on the final text of the legislative proposal has been reached and both the Parliament and the Council have formally adopted it. After being published in the Official Journal of the EU, the Data Protection Regulation will enter into force and must be applied in all EU Member State following a two-year transition period.



LOBBYING

and the Data Protection Regulation

Politicians must rely on expertise in order to make decisions across an extremely broad range of areas. The boundaries between merely providing information and attempting to exert an influence are fluid. The reorganisation of EU data protection is one of the most extensive legislative proposals in the history of the European Union. This is reflected in the amount of lobbying on this reform. In the multi-level European institutional system, lobby groups and associations have a wide range of opportunities to exert an influence: during the consultation pro-

cess before a Commission proposal is published, by contacting MEPs in key positions or by maintaining good relations with the Permanent Representations, i.e. with the Member States' embassies to the EU.

On the one hand, knowledge and expertise can assist Members in their parliamentary work. Since an extremely diverse range of interests is often involved, lobbying may also be understood as a form of feedback on the interests of different social groups. On the other hand, politicians also need to be able to verify and weigh up lobby proposals. Unquestioningly accepting formulations written by outside parties casts doubt on the independence of political decisions. The information provided may be deliberately misleading, incomplete or selective. Fabricated studies are not uncommon, such as that study on “the economic importance of getting data protection right” by the U.S Chamber of Commerce. This claims that expanding the already existing right to be forgotten through this reform would cost each household EUR 3,512. A clear imbalance is apparent in the influence exerted: business interests dominate, as social and ecological interest groups do not have as much money to push through their agendas.

The Data Protection Regulation is a good example of how far a law can become the plaything of commercial interests. We can gauge the influence of lobbies thanks to the crowdsourcing platform www.lobbyplag.eu: the Berlin-based Open Data City project shows which amendments were proposed by lobbies and submitted as such verbatim by MEPs. As rapporteur, Jan Philipp Albrecht disclosed his meetings with businesses and associations. The dominance of commercial lobby groups through ex-

tremely frequent requests for appointments, invitations and meetings clearly illustrates the attempt to influence the political decision-making process. Available (in German only) at: <https://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/lobbyismus-zur-eu-datenschutzreform.html>.

Anyone wishing to find out exactly which MEPs submitted which phrases as amendments to the Data Protection Regulation can find a list here with evaluations made from the point of view of data protection: <http://lobbyplag.eu/map>.

You can check which passages MEPs copied from interest groups here: <http://lobbyplag.eu/influence>.

The “[Activist Guide to the Brussels Maze](#)” brochure produced by EDRI (European Digital Rights) is a useful starting point for activists seeking to gain influence: https://edri.org/files/activist_guide_to_the_EU_2012.pdf.

The platform LobbyCloud wishes to tackle the information and transparency deficit in the legislative process. Lobby documents can be uploaded anonymously and made available to the public. Interested parties can use it to see who has influenced whom: <https://lobbycloud.eu>.



How can I protect **my privacy** on the internet?

Strong passwords are passwords which include random combinations of letters, numbers and special characters, have at least twelve characters, and do not include your own name or the name of your pet or best friend. Passwords should never be given to anyone and should be changed regularly. The same or a similar password should be not used for different accounts. Password managers such as the open-source and freely available KeePass store all passwords in an encrypted database.

Private e-mail inboxes: European providers such as posteo.de or mailbox.org offer publicity-free inboxes. E-mail content is not analysed for advertising purposes.

Encryption: Pretty Good Privacy (PGP) and the free version of GNU Privacy Guard (GnuPG) are successful providers of e-mail encryption. The Enigmail plugin for email software such as Thunderbird facilitates encoding, decoding and key management.

Instant messaging: For instant-messaging free, decentralised services such as Jabber (xmpp) can be recommended. These are available to use on both PC and smartphone, ideally with OTR standard encryption. For Android there is the Jabber app Chatsecure. Text messages can also be encrypted, for example with Textsecure. Other alternatives include Surespot and the fee-based Threema.

Masking IP addresses: IP addresses can be masked using the free software Tor (The Onion Router) so that online services do not know who is accessing them and from where. Warning: Tor only conceals the origin, not the content of data. Additional HTTPS-encrypted communication is therefore also required, for example when entering login details.

Using HTTPS: HTTPS is the encrypted version of the internet protocol HTTP. The HTTPS-Everywhere expansion for Firefox and Chrome enables users to surf websites using an HTTPS connection where possible.

Advanced anonymous internet surfing: Tails (“[The Amnesic Incognito Live System](#)”) is a free operating system offering maximum anonymity when surfing the internet. Tails can be launched from a USB stick, a DVD or SD card on any computer, regardless of the operating system. Data is not stored on the computer’s hard disk but on the working memory, which is then deleted from the device after it is shut down. User guidelines and the current version are available for download at [tails.boum.org](#).

File hosting: Dropbox is a popular Cloud hosting service. However, the service is questionable in terms of data protection: unencrypted data is readily passed on to the US government. Alternatives include Teamdrive, developed in Hamburg, or the services Pulse, Wuala and SpiderOak. Those who are ambitious can also set up their own cloud with the open-source-project OwnCloud.

Search engines: There is more than just Google. Many other search engines are more careful with personal data: ixquick, DuckDuckGo, yandex.com or YaCy.

Term and conditions of use: The voluntary platform Terms of Service; Didn’t Read analyses the small print. General terms of business are broken down into easy-to-grasp tips. Colour icons make it possible to identify the disadvantages of a service straight-away. Here again there is a Firefox tool available. The awareness-raising campaign [biggestlie.com](#) explains why concise and understandable terms and conditions are so important.

Browser cookies: Cookies are practical, however they also reveal a lot about an individual’s surfing habits. Doing without cookies completely leads to limitations, since many things on offer can only be used when cookies are activated. With the Self-Destructing Cookies expansion (Firefox), cookies are automatically deleted after a web page is closed.

For more information, see:

<https://securityinabox.org>.

<https://myshadow.org>.

<https://digitalcourage.de/adventskalender> (in German)

Jan Philipp Albrecht, MdEP
Platz der Republik 1
UDL 50 – 2113
11011 Berlin
Germany



jan.albrecht@europarl.europa.eu
www.janalbrecht.eu
twitter.com/janalbrecht
youtube.com/ JPAforMEP

A free printed version of this brochure can be ordered at info@gef.eu

Photo credit: archiv/private; Glassball, pile of documents, hand, speakers, heart, mouth, ear, brain, eye © istockphoto.com; Photo Jan Philipp Albrecht © Valentina Vos; Euro notes, USB cable, broken glass, glassball 2, people © Shutterstock; Test tubes - Africa Studio © fotolia.com; TPunchcard © Harke - CC BY-SA 3.0

