



Europe comes of **DIGITAL AGE**

.....
"EU Data Protection Reform"

A BCCD White Paper
Business and Politics Series
June 2016



Foreword

Giovanni Buttarelli European Data Protection Supervisor

All over the world business and public authorities are gradually coming to terms with a new legal reality. Data protection is no longer one specialism among many for legal compliance teams; it is becoming an issue for the whole organisation from production to purchasing, from HR to R&D, and even at Board Room level.

So I am delighted that the British Chamber of Commerce in Denmark has chosen this topic for its latest White Paper.

In May of this year, after perhaps the most intense, prolonged and complex negotiations over a single piece of EU legislation ever, the European Union adopted the General Data Protection Regulation and the Data Protection Directive covering the criminal justice and law enforcement areas – these instruments are the first of a new generation of data rules for the digital age. It will be closely followed by the modernisation of the Council of Europe’s Convention 108, which has been in place since 1981.

Denmark has a long term tradition of defending and promoting human rights. Denmark is also the leader among the 28 EU Member States according to the Commission’s indicators of digital economy and society. Danes are the most sophisticated internet users, from banking to shopping to social media. This country has also been at the front line of defending values such as freedom of expression, especially in the wake of the shootings in this city in February last year. In Denmark, as in other Member States, there is

fierce debate about the necessity and proportionality of surveillance activities and security measures in the light of these threats.

Data protection issues are global issues. There have been plenty of headlines in recent months on the effort of the EU and the US to agree a Privacy Shield covering transfers of personal information to the US for commercial purposes. This is of course a vital strategic consideration. But let us not forget that globalisation means much more than the EU and the US. Under the GDPR, companies will be accountable for all personal data processing - not just transfers to countries outside the EU.

For all of these challenges, whether concerning commercial practices or security, the role of supervisory authorities is more indispensable than ever. In the Charter of Fundamental Rights of the EU – primary law on the level of a state’s constitution - compliance with data protection rules must be subject to an independent authority. This is an ‘essential component’ of data protection in the EU, a “sine qua non”. In the last few years, the CJEU has provided great clarity on what this independence means. In three separate cases concerning Germany, Austria and then Hungary, the Court has affirmed that:

- data protection authorities, whether or not logistically attached to government offices, must be independent directly and indirectly from government and other public institutions influence which may affect decisions;

- authorities, even if they do not have an independent budget, must be above all suspicion of their independence being ever compromised; and
- authorities cannot be replaced during term of office in violation of applicable rules and safeguards. Such a move is tantamount to removing a judge.

In fact the Court implied that the institution I lead, the European Data Protection Supervisor, as set up under Regulation 2001/45, was a model for how data protection authorities should be established. That Regulation will also be reformed in the next year or so.

Data protection authorities exercise this independence in all their functions, from investigating and intervening in risky or potentially unlawful processings to bringing violations to court; from handling individual complaints to providing advice on legislative and technological developments. In other words, we are ombudspersons, auditors, consultants, educators, negotiators, policy advisers and enforcers.

The new Regulation invests authorities with stronger powers and responsibilities, most notably in the area of sanctions for violations of the Regulation. On top of all of this, it introduces detailed requirements for cooperation between authorities, including cooperation on cases (Art. 60), providing information and assistance (Art 61), inclusivity and

joint investigations (Art. 62), cooperating through consistency mechanism (Art 63), sharing key decisions on data protection impact assessments, standard contractual clause and binding corporate rules (Art. 64) and communicating all urgent measures to the new coordination mechanism, the European Data Protection Board (the 'EDPB') (Art. 66).

With these tasks comes accountability towards individuals and towards controllers, the business and other organisations who need to handle personal information. We data protection authorities individually and collectively must be responsive to developments, accessible, efficient in dealing with issues and openly and sincerely consider the views of stakeholders when exercising our enforcement powers and producing guidance.

My institution will fully engage with this process, as an independent authority and a member of the EDPB, and as the provider of the secretariat to this Board.

Data protection and privacy laws have proliferated all over the world, and that is largely thanks to the leadership of the EU. In the words of a one scholar, EU law is the 'engine of a global regime', raising standards around the world not aggressively but through a sort of non-coercive, persuasive soft law.

That is something that Europe should be proud of.



Table of content

The Issue – The EU’s Digital Reform

- 8 “Casting a dragnet rather than a fishing line”

Rounded Perspectives

- 10 The GDPR: Burden or opportunity?
- 13 Supporting the EU-US Privacy Shield
- 16 Building trust in the digital age
- 18 The Privacy Shield and GDPR – Legal Certainty Going Forward?
- 20 The next challenge for European Privacy Policy Frameworks – adherence to Better Regulation Principles!

Conclusion

The value of the BCCD Business and Politics forum





Don't just fly. Fly First.

Stretch out and unwind in privacy. Your comfortable First seat converts into a fully flat bed at the touch of a button.

Discover more at [ba.com/first](https://www.britishairways.com/first)

“.. we are now faced with a new reality, where data and even more so data protection are going to be determining factors in competitiveness.”



EU Data

“Privacy Shield”

10 MAY 2016, H



MAIN EVENT SPONSOR





Mariano A. Davies
President & CEO



Jens Klarskov
CEO, Confederation of Danish Enterprise

Executive Summary

The British Chamber of Commerce in Denmark and the Confederation of Danish Enterprise in co-operation with the European Commission organized the world's first-ever international conference on the General Data Protection Regulation (GDPR) on 10 May 2016 in Copenhagen.

The event brought together key policy makers, industry leaders and consumer rights experts to discuss not only the implications of this far reaching piece of legislation from Brussels, but also the new EU-US Privacy Shield arrangement for transatlantic transfers of personal data.

Both our organizations see this as a substantial achievement and a huge opportunity for European companies to grow.

Data is the new oil. It is a raw material that is going to fuel our economy and take it to new levels. The data-driven economy has already taken off, but we are going to see fundamental changes and new business opportunities in the future. Data is no longer limited to the IT-industry, on the contrary all sectors of our economy are increasingly becoming dependent on data. This is also the case for global trade. Whenever goods and especially services are traded across boarder, they are accompanied by data flows. These flows are increasing and, in this ever more interconnected world, are essential for growth and job creation in Denmark, UK, EU and beyond.

Although data is a tremendous resource full of potential, it must be handled with care. This is why we both as heads of our respective organizations are welcoming the results of the EU institutions hard work to establish a new rule book for handling data.

Getting it right will be an important step in the right direction, however, as the EU is entangled in a global

flow of data, the GDPR is not enough on its own. This is why the Privacy Shield is paramount as well. The economic importance of the data flows across the Atlantic cannot be underestimated. Cutting them off would be like cutting off the electricity. Of course our European clients' personal data should be kept safe and their rights honored also when the data is transferred to the USA. This fosters trust in the global data-economy and this is why we strongly support the Commissions in its efforts to negotiate an ambitious agreement on the Privacy Shield.

At the conference, the EU Justice Commissioner, Vera Jourova, the European Data Protection Supervisor and the US Deputy Assistant Secretary of Commerce, Ted Dean, underlined the fact that both document will redefine how businesses collect, process and transfer the personal data of EU citizens in Europe and across the Atlantic.

Industry leaders like John Frank of Microsoft, Amit Bajaj from Tata Consultancy Services and Ulf Pehrsson from Ericsson took turns in analyzing the new regulations. We encourage you to read their contribution to this paper. See next articles.

The key take away from the conference was that we are now faced with a new reality, where data and even more so data protection are going to be determining factors in competitiveness. If we get it right in the EU, European companies have the chance to gain a competitive edge by being on the forefront when it comes to protecting more and more privacy conscious consumers.

Last but not least, we would like to thank all our partners for making this conference possible. We look forward to seeing you all again at other occasions.

We hope you will enjoy reading this paper.

Mariano A. Davies
President & CEO

Jens Klarskov
CEO, Confederation of Danish Enterprise



Deo Delaney
 Head of Business Dev,
 EU and International Trade,
 British Chamber of Commerce in Denmark

The Issue: The EU's Digital Reform

“Casting a dragnet rather than a fishing line”

The General Data Protection Regulation (GDPR) marks the beginning of a new era in Europe, with rules and regulations fit for the digital age. With the new legislation intended not only to strengthen EU citizens' rights but also to simplify rules for businesses in EU Member States, every EU citizen is a vital stakeholder in the process.

Data flows are increasingly at the heart of modern economies, as demonstrated not only by the adoption of the GDPR but also the completion of the EU-US Privacy Shield Agreement, covering data flows between the EU and its largest trading partner. These sweeping changes regarding citizens' data reflect the growing importance of personal data; as the Former Vice-President of the European Commission Viviane Reding put it back in 2012, “Data is at the centre of the digital world. It is the currency of this new market”. In this context, there are three issues that both documents cover which I would like to highlight here.

First, the new legislation is broad-based covering 28 Member States, replacing the patchwork of individual legislation that was previously in place. This has given rise to concerns regarding the interpretation and its consequent implementation. A key feature of the GDPR is the vague nature of certain sections, allowing space for interpretation. Although a minimal amount of divergence at a local level is impossible to avoid due to the differences between Member States, it is important to reach a standard on common areas across the EU. If there is too much divergence between the Member States' applications, the full potential to unlock the benefits of the EU Digital Single Market will not be attained.

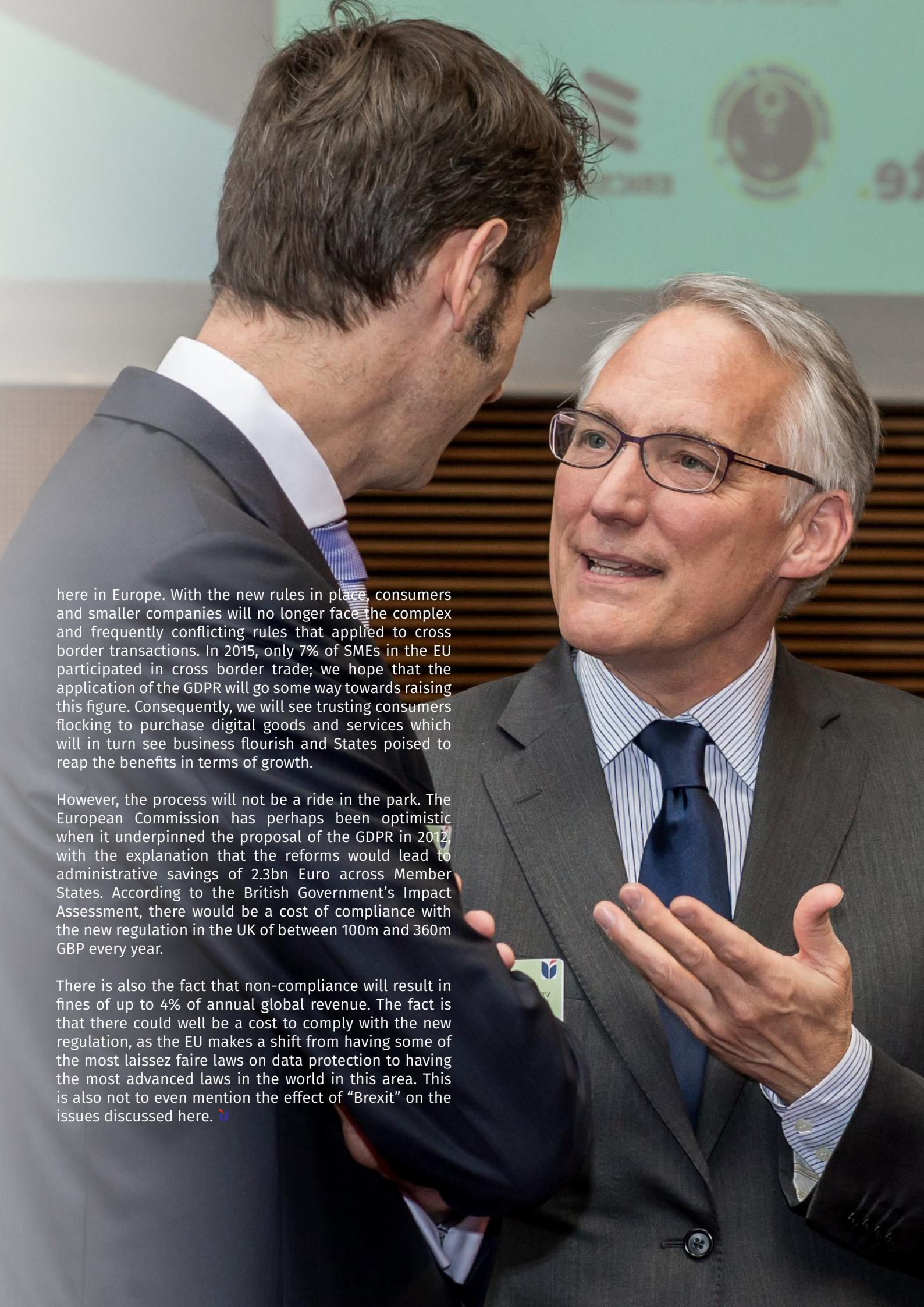
One example of differing interpretations is the concept of “legitimate interest pursued by a controller” in Article 6 (1f), which is one of six possible grounds for lawfulness of data processing. The definition of what constitutes a

“legitimate interest” could vary considerably in different Member States. In this way, the GDPR could be likened to casting a dragnet covering a wide area but it means collecting a lot of unwanted material alongside the coveted targets.

Second is the importance of consumers trust, tied to the fundamental right to privacy. Citizens must trust in both businesses and governments, that valuable personal data will not be used for any purpose other than that which the data subject intended. The fundamental right to privacy yet presents an opportunity for businesses to ensure that the concept of “privacy by design” is embedded into any new product that enters the market.

There is much to gain for businesses that manage to do this, as they can both demonstrate compliance with the regulation and create a competitive advantage at the same time. Microsoft for example, has understood this, with Vice President John Frank explaining that “our business is built on trust”. The companies that provide the clearest proof of this stand to benefit the most.

Third and finally, these regulations unlock the benefits of a harmonized EU Digital Single Market. European Commission President Juncker declared to the European Parliament in 2014 that “if we are successful in implementing a real digital single market we, can generate 250 billion Euro of additional growth in Europe”. The adoption of the GDPR is an important step in accelerating the trend for future e-commerce



here in Europe. With the new rules in place, consumers and smaller companies will no longer face the complex and frequently conflicting rules that applied to cross border transactions. In 2015, only 7% of SMEs in the EU participated in cross border trade; we hope that the application of the GDPR will go some way towards raising this figure. Consequently, we will see trusting consumers flocking to purchase digital goods and services which will in turn see business flourish and States poised to reap the benefits in terms of growth.

However, the process will not be a ride in the park. The European Commission has perhaps been optimistic when it underpinned the proposal of the GDPR in 2012, with the explanation that the reforms would lead to administrative savings of 2.3bn Euro across Member States. According to the British Government's Impact Assessment, there would be a cost of compliance with the new regulation in the UK of between 100m and 360m GBP every year.

There is also the fact that non-compliance will result in fines of up to 4% of annual global revenue. The fact is that there could well be a cost to comply with the new regulation, as the EU makes a shift from having some of the most laissez faire laws on data protection to having the most advanced laws in the world in this area. This is also not to even mention the effect of "Brexit" on the issues discussed here. 🇪🇺



Jeppe Brogaard Clausen,
Partner, NJORD Law Firm



Niels-Peter Kjølbye
Attorney, NJORD Law Firm

Rounded Perspectives

The GDPR: Burden or opportunity?

The newly adopted GDPR will bring increased harmonisation to data protection regulation in the EU from summer 2018. For the consumers this is good news, as their rights as data subjects will become more transparent and will be enforceable towards all companies established or offering services in the EU. For companies, the rules represent increased requirements to legal compliance. Does that represent a burden or an opportunity? Here is our reflection on the new rules.

Consumers or other data subjects rarely hesitate to submit personal data as long as it is logical and for their own benefit. The crucial point is how companies use and manage the data and that the data subjects can get access to information about themselves, have data updated or deleted and transfer the same data to another vendor if wanted.

With the GDPR's clear and harmonised rights for data subjects, companies will compete based on privacy in the future, and consumers will undoubtedly choose the options, which give them the better data protection. If companies get it right, they may even learn that there are new business opportunities waiting to be exploited.

Some of the key elements in the GDPR are that

- data controllers shall use easy-to-understand language towards data subjects (transparency),
- data controllers shall make it possible for the data subjects to have their data deleted (the right to be forgotten),
- the data shall be portable meaning that it can be transferred by ordinary electronic means (portability),
- the collection and processing of data shall take place with a minimum of means taking into account all circumstances (privacy by design),

- data controllers shall appoint a data protection officer (DPO),
- data controllers shall be able to document that they are compliant (accountability), and
- fines are increased severely and can be expected at a level of up to 4 % of global revenues.

There are exemptions for Small and Medium Sized Enterprises (up to 250 employees), and the rules will in the next two years be subject to various interpretation and guidance. However, it is generally clear that all data processing shall be fair and transparent, and that the measures taken towards protection of the data shall fit the nature and use of the data. The burden of proof lies with the data controller (the company deciding for which purpose data is collected and used).

“With the GDPR's clear and harmonised rights for data subjects, companies will compete based on privacy in the future.”

On this basis, we believe that the companies which are able to adapt to principles as “privacy by design”, the companies which are able to weigh their own interest



with individuals' rights, and the companies which are able to efficiently manage customer data requests and complaints, will be able to compete based on privacy. If companies are not able to do that, they will fall behind in competition.

Starting with a data flow analysis of their own business, companies may begin getting ready for the new rules now. This will minimize the risk of fines in two years, but more importantly, it will be possible to get a head start of competitors. A data flow analysis could for example consist of the following:

- What kind of data is collected? (Employees' data, customer data, health information, etc.)
- On what grounds has the data been collected? (Consent from the data subject, agreement with 3rd party, legal requirements)
- What is the data used for? (HR management, answering requests from customers, profiling, marketing, research and development)

- Where is it stored? (local server in Denmark, cloud service in the US, headquarters in Germany, subsidiary in China)
- Who has access? (All in your business, HR management, cloud-service provider, subsidiaries, etc.)
- For how long is it stored? (When will it be deleted and who can do it?)

From this exercise, companies may actually get to know their business a lot better. For example, companies may find that they have data, which they did not think they had, and which may be used to explore new business opportunities or interconnections with the present business activities, making it possible to boost sales or marketing efforts.

All companies with more than 250 employees or for which data processing is at the heart of their business are therefore advised to prepare themselves without waiting for the GDPR to enter into force in summer 2018. There may be plenty of opportunities to be grasped along the way. 🇩🇰



Global Analysis for Better Decisions

A world leader in economic forecasting and quantitative analysis, Oxford Economics offers a portfolio of briefing reports, databases and analytical tools on a subscription and consulting basis.

- Rigorous quantitative economic forecasts for over 200 countries and 100 industries
- City and regional forecasts for over 3000 global locations
- Evidence-based analysis and public policy advice, supporting business, policy and market decisions

For more information,
contact Jens Tholstrup at
jtholstrup@oxfordeconomics.com
or call +44 207 803 1439.





John Frank
VP EU Government Affairs,
Microsoft

Supporting the EU-US Privacy Shield

In light of the ongoing discussions about the EU-U.S. Privacy Shield – the framework to replace the Safe Harbor agreement that governed data transmission between Europe and the United States until it was overturned last October – I want to share an overview of where Microsoft stands in this important debate.

First and foremost, at Microsoft we recognize that privacy is both a fundamental human right and an issue about which our customers care deeply. In a time when business and communications increasingly depend on the transmission of personal data across borders, no one should give up their privacy rights simply because their information is stored in electronic form or their technology service provider transfers it to another country.

Europe’s data protection regulators have recently made some recommendations for ways in which the Privacy Shield can be strengthened even further. We encourage the European Commission (EC) and the U.S. Department of Commerce (USDC) to consider them. We don’t believe these changes will require a re-opening of the Privacy Shield, but rather clarifications of its current.

As a company, we’ve also said since last fall that no single legal instrument can address for all time all of the privacy issues on both sides of the Atlantic.

We believe that the EC and USDC deserve credit for addressing complicated legal issues in ways that create stronger and pragmatic privacy protection for European citizens while enabling the continued movement of data that is the lifeblood of our economies.

We also recognize that the effectiveness of the Privacy Shield will turn in part on the responsible steps taken by companies to abide by it. Last April, I had the privilege

to announce Microsoft’s pledge to sign up for the Privacy Shield.

Part of Microsoft’s commitment, as the Privacy Shield envisions, will be to respond promptly to any individual complaints we receive. Specifically, we’ll do this within 45 days. In addition, Microsoft will commit to cooperate with EU national Data Protection Authorities and comply with their advice as regards any disputes under the Privacy Shield.

.....
“This focus on privacy reflects not just our belief in fundamental rights and the rule of law, but also our understanding that our business is ultimately built on trust.”
.....



We also welcome the obligations in the Privacy Shield for transparency about government requests of access to personal information. As a company we have advocated for greater U.S. transparency, and we are gratified that the Privacy Shield addresses this issue directly. In 2013, Microsoft and other U.S. tech companies successfully challenged the U.S. Government over our constitutional right to disclose more detailed information about the Government's demands for data. And in 2014, we filed suit against the U.S. Government after it attempted to force us to turn over a customer's email stored in our Irish data center. While we continue to advocate for additional domestic legal steps in the United States, we believe that the EC and USDC have chosen a sensible approach in the Privacy Shield that introduces safeguards for European data to supplement those in U.S. law.

We are also committed to doing our own part as a company to provide citizens in the EU and worldwide with information about our practices as a company. We will therefore continue to maintain the highest levels of transparency about government requests for access to personal information. Our Law Enforcement Requests Report (which we started in 2013) and our U.S. National Security Orders Report (which we started in 2014) appear twice a year.

Microsoft's commitment to privacy has been proven by our actions. We were the first enterprise cloud services provider to implement the rigorous controls needed to earn approval for our contractual model clauses governing the transfer of data outside of European Union. We were also the first cloud provider to achieve compliance with ISO's important new 27018 cloud privacy standard. This focus on privacy reflects not just our belief in fundamental rights and the rule of law, but also our understanding that our business is ultimately built on trust.

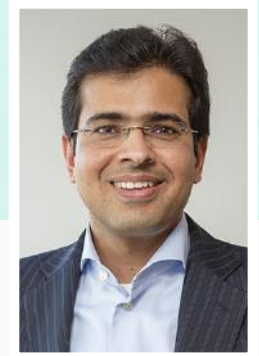
We're entering a remarkable period in the history of technology development as cloud computing connects people around the world to advanced capabilities that have the potential to drive economic growth and address some of the world's most pressing challenges. But people won't use technology that they don't trust. By providing a clear framework that ensures key protections of EU citizens continue when data is transferred to the United States, the Privacy Shield framework is an important step in enhancing trust in the global digital economy, and we hope that it will be agreed and approved quickly, adopted broadly by organizations and supported by stakeholders. 🇺🇸





D'ANGLETERRE

COPENHAGEN
EST. 1755



Amit Bajaj
Head, Northern Europe,
Tata Consultancy Services

Building trust in the digital age

The advent in 2018 of the General Data Protection Regulation is an initiative of immense importance both societally and technologically. Its roll out across the EU's member states will reinforce the data privacy rights of individual citizens and at the same time introduce stringent rules for companies and organizations that handle their personal data.

Considering how reliant our digitized society has become upon unimpeded data flow, this Regulation is nothing short of a revolution.

But as with all revolutions, the work begins immediately afterwards. In this case, however, is expected that the bulk of the work to develop these guidelines will be carried out during the first year after the Regulation enters into force (i.e. between April/May 2016 and April/May 2017). Whilst the Regulation should ensure greater uniformity of the rules, for it to work it must be applied in the same way across the EU as was intended.

Is innovation under threat?

Equally important is the Regulation's impact on business – in particular, its effect on innovation and competitiveness which is so vital to the success of the EU as an entity and the way in which private individuals' data is handled in the pursuit of business. Will companies be able to continue to access and process data while complying with legal requirements and will companies be able to continue offer tailored services using profiling of users? These are all legitimate questions.

Industry reaction has been predictably wary taking into consideration the extra layer of complexity in compliance in addition to the harsh sanctions for non-compliance. With respect to innovation, it is clear that clear channels of communication between industry and policymakers need to be established during the


implementation phase to find practical and creative solutions for meeting the new obligations.

The need for security and trust

In the key area of data security, the need by companies processing data to perform a data protection impact assessment if the processing is likely to carry a high risk for individuals' rights and freedoms is particularly relevant in the banking and financial industry. Data breaches could result in financial loss or identify fraud for data subjects which would clearly run counter to the ambitions of the Regulation.

Indeed, taken on a higher level, what we are dealing with are issues of trust and security between business and government, and the rights of individual citizens. As a technology company that works with both private business and the public sector, we are actively developing solutions that will foster new levels of trust and security between all three sets of stakeholders.

“Considering how reliant our digitised society has become upon unimpeded data flow, this Regulation is nothing short of a revolution.”



One solution, among others, which we hope addresses some of the bigger concerns about data privacy we have called, not inappropriately, Crystal Ball - a platform which acts simultaneously as an observer and enforcer at the service level between organizations and their customers' data. Using a technique called Role Based Masking, Crystal Ball records and audits how individual pieces of information are exposed to various members of an enterprise in the process of a transaction. Protocols inherent in this solution may also be included to directly ask permissions from consumers about their individual data exposure. This will go a long way to enabling regulatory compliance for both individuals and the organizations that serve them.

As a firm advocate of individual rights but also business, I believe that GDPR is not just about compliance but for those who truly embrace it, it can also be a source of competitive advantage. The newly defined rights for data subjects, such as the right to data portability provides a clear business opportunity as companies adapt their systems to allow for data to be exported in usable formats. This also applies to provisions on 'data protection by design and by default' which would require data processing systems to be built around the new data protection rules.

Giving customers and simultaneously EU citizens the transparency & control of their data is the source of earning "trust" in the digital age. As a currency in business, it supersedes all others. 🍀



Maarten Meulenbelt
Partner, Sidley Austin LLP,
Brussels

The Privacy Shield and GDPR – Legal Certainty Going Forward?

The spring of 2016 will be remembered as one of the most important times of development in EU data privacy law.

The adoption of the General Data Protection Regulation (GDPR) last month was an important step that reminds us of the biggest benefit that EU laws can bring to businesses: the opportunity to reduce red tape. Not so much by abolishing red tape, but by reducing the *duplication* of red tape. The streamlining of European authorisation processes for medicinal products can provide a positive example on this point. Of course, the GDPR did not fully succeed in establishing a “one stop shop” for businesses currently dealing with dozens of national and regional Data Protection Authorities. However, the GDPR will reinforce coordination between Data Protection Authorities and we hope that further harmonisation and streamlining will be achieved by the Article 29 Working Party, the European Data Protection Supervisor, the European Commission and others working hard to establish implementing rules and set up the European Data Protection Board.

The GDPR brings much that is new, but also confirms much of what we have already. That brings me to the Privacy Shield, which is the second key development this Spring.

The Privacy Shield, as we all know, is a response to the Schrems judgment in which the Court of Justice invalidated the Commission’s 2000 Safe Harbour Decision. The key thing to note about the Schrems judgment is that this judgment has a limited scope. The Court of Justice invalidated the Safe Harbour Decision because that Decision did not address the rules that exist in the U.S. to limit government access to personal data. The Court also gave guidance to the Commission for future Decisions replacing the Safe Harbour Decision. Such future Decisions may not permit transfer to third countries if such transfers would lead to “storage of all the personal data” of all Europeans “without any differentiation, limitation or exception”, and without rules “to determine the access of the public authorities”.


The Court also condemned government “access on a generalised basis” as well as “legislation not providing for any possibility for an individual to pursue legal remedies.” In other words, there must be proper safeguards. The Court, however, did not investigate any facts (that is not its job) and did not conclude that U.S. laws cause exposure without proper safeguards.

The Privacy Shield negotiators did a remarkable job of mapping the key U.S. laws which already provide safeguards for data transferred to the U.S. (and I would like to recall that those laws were not reviewed by the Court of Justice). The negotiators supplemented those protections with a series of documents from U.S. authorities that explain the enforcement regime in the U.S. regarding the protective commitments that Privacy Shield companies would sign up to, the limitations to U.S. government surveillance, as well as the inventive step of establish the Ombudsperson that will deal with complaints.

.....
“...the GDPR will reinforce coordination between Data Protection Authorities and we hope that further harmonisation and streamlining will be achieved...”
.....

There is little doubt that the Privacy Shield, if adopted, will lead to new cases before the Court of Justice. But that risk also applies to other solutions used by thousands of businesses since the Schrems judgment, and notably to “Standard Contractual Clauses” or “Model Clauses” which are still in force: several DPAs have suggested that Model Clauses should not be used as a basis for transfers to the U.S. because of exposure to U.S. surveillance.





There are reasons to be hopeful that significant parts of the legal framework permitting transatlantic data flows will withstand these new challenges. First, for cases that require a general assessment of the level of protection in the U.S. - such as the Privacy Shield - we can draw upon the guidance provided by the case law of the European Court of Human Rights, which explains that Member States have a 'margin of discretion' regarding surveillance: they must balance the sense of unease that comes from terrorist threats with the sense of unease that comes with 'being watched'.

Thus, far-reaching surveillance must be accompanied by far-reaching safeguards against abuse. That, as a group of colleagues and I set out in Sidley's Essentially Equivalent report of January 2016, is a key part of the "EU Benchmark" that the U.S. must meet under the Privacy Shield, and in our view that benchmark is met. Second, for individual cases involving actual company data flows, businesses can require DPAs and national courts to assess the actual level of risk for the data they are handling. DPAs and courts should not block data flows unless there is actual risk. 🌱



Ulf Pehrsson
Vice President,
Head of Global Government Relations, Ericsson

The next challenge for European Privacy Policy Frameworks – adherence to Better Regulation Principles!

In the coming decade, 90 percent of global GDP growth is expected to take place outside the EU. Coupled with the OECD’s proclamation that data-driven innovation will form a key pillar in 21st-century sources of growth, the European project stands at a critical economic juncture. Mobility, broadband, cloud, big data and analytics, which are all essential elements of data-driven innovation, are rapidly becoming the core assets of a digital economy.

Europe is rightly proud of its knowledge-based society and economy. However, the continent’s future prosperity is at great risk if the European Commission’s well-intentioned and self-imposed Better Regulation principles continue to be sidelined in the formulation and implementation of the EU’s privacy policy frameworks.

Data-driven innovation is swiftly changing our understanding of what the internet is all about. The preconception that it is primarily a consumer experience anchored in the Web 2.0 paradigm is being reshaped into the concept of a disruptive, transformative force that enables industry digitisation, the Internet of Things, Industry 4.0, smart cities, e-health and so on. Information & Communication Technology (ICT) is therefore becoming a **fundamental** condition for creating value and benefits in most sectors of today’s economies. As a result, the stakes for societies engaging with ICT are now much greater and more far-reaching than the mere satisfaction of consumers’ immediate needs and wants.

Of course, consumers will not disappear and they will continue to be important. However, as the new frontiers that characterise digital economies and societies reshape Europe’s industrial foundation, we – including privacy policy makers – will need to consider people not just as consumers but equally acknowledge and support their needs and rights as citizens, employers, employees, patients, commuters, city dwellers, students and so on.

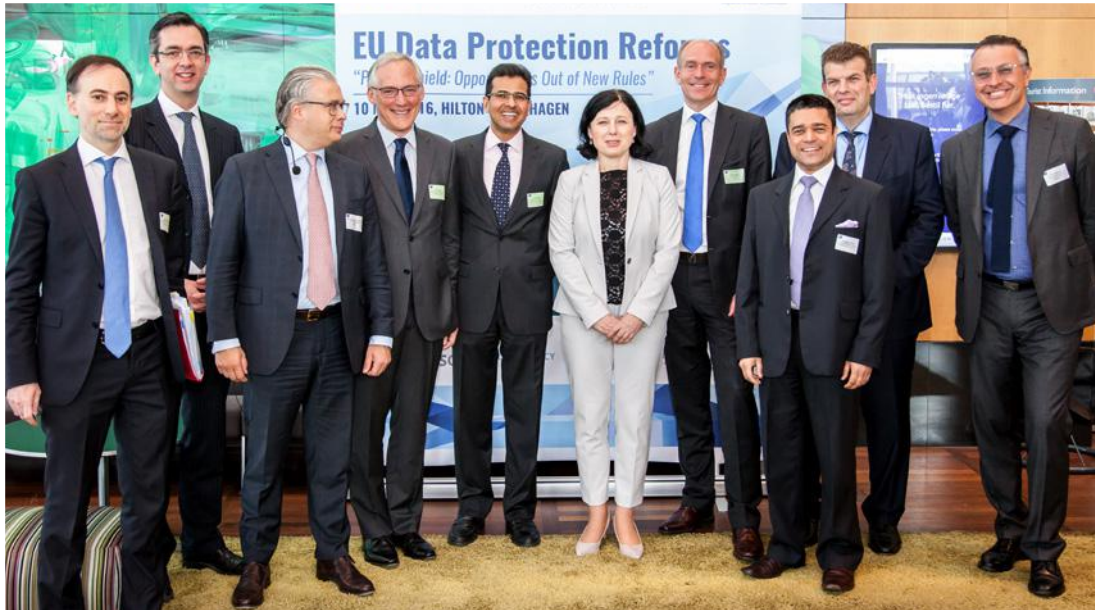
We can all recognise that a successful digital economy and society is one that knows how best to use information and knowledge to achieve the full spectrum of its desired ends and goals. But the current European privacy policy debate is de facto pursuing just one goal – the right to privacy. This tunnel vision persists in spite of the fact that although the right to privacy is a fundamental right, it is not an **absolute right**. In the handbook on European data protection law, one can read that: “The fundamental right to the protection of personal data under Article 8 of the Charter is not, however, an absolute right, but must be considered in relation to its function in society.”

The threat to Europe’s digital economy

This tunnel vision is a key limiting factor that seriously hinders the development and implementation of progressive privacy policies that live up to the standards of Better Regulation principles while achieving the fundamental goal of protecting privacy. In consequence, it threatens Europe’s path to future prosperity in the digital age. As 19 EU Ministers have recognised, these principles should be understood in the following way:

*“[W]e recognise the need to address the quality of EU legislation as well as to reduce its overall regulatory burden, without undermining its policy goals. This must include both the existing acquis and new proposals in order to ensure that EU regulation is transparent, simple and is **achieved at minimum cost, while fostering competitiveness, growth and jobs.**”*





To clarify my point, I would like to give three examples of policy makers falling prey to tunnel vision and thereby sidelining the possibility of privacy policy frameworks living up to Better Regulation principles.

- **In the form of rhetoric:** statements to the effect that more and more privacy regulation will increase the competitiveness of European companies are built on a logic implying that an increase of regulation will make companies more competitive. No compelling evidence has yet been advanced to back up this rhetoric, and neither experience nor economic theory support it.
- **In the form** of an attitude: when business challenges some privacy proposals, this is frequently dismissed and labeled as being contrary to the fundamental right to privacy. This is a very effective way to block the emergence of constructive, balanced and progressive privacy policy legislation, while preserving a one-sided policy approach.
- **In the form** of substance: Europe's need for better and smarter regulation – as expressed by the Member States Ministers – must be extended to the privacy policy making domain and be well reflected in the work of key stakeholders such as DG Justice, the EDPS and the future EDPB. In this context, I would welcome a new central, well-observed function with a clear Better Regulation

mandate that covers the beginning of the policy formulation process as well as implementation in EDPS and/or EDPB – **possibly in the form of a Chief Economist**. This will help ensure Better Regulation principles are fully reflected in the privacy policy debate.

.....

“Mobility, broadband, cloud, big data and analytics, which are all essential elements of data-driven innovation, are rapidly becoming the core assets of a digital economy.”

.....

Technology – no matter how innovative – cannot be expected to digitise Europe's knowledge economy on its own. Policy makers have a decisive role to play: one that will either suffocate technological development or drive a new wave of modernisation and prosperity. We must remind ourselves of Manuel Castells' observation:

“If society does not determine technology, it can, mainly through the state, suffocate its development. Or alternatively, again mainly by state intervention, it can embark on an accelerated process of technological modernization able to change the fate of economies and social well-being in a few years.” 🇵🇹





Michael Vedsø
Acting Head of Office,
EU Representation in Denmark

Conclusion

Privacy Shield is a ground-breaking step forward in US-EU business relations. As rich and developed societies, both the US and the EU have very high potential gains ahead: data is the currency of the future, business growth in this area promises to create wealth and jobs on both sides of the Atlantic.

For this to happen, the first requirement is a stable and predictable regulatory environment. This is exactly what Privacy Shield represents. Both the US and the EU side are to be commended for reaching an agreement on this technically complex and legally sensitive area.

It will now be for businesses to build projects on this stable and agreed platform, which offers consumers and everyone else high standards of data protection. The Copenhagen Conference reaffirmed the huge potential from the business perspective, which suggests that this regulatory platform can deliver on our expectations for jobs and growth.

Yet, we must not forget the fundamental reasons for establishing the Privacy Shield: protecting personal data and respecting citizen's right to electronic privacy is an ethical question, which reaches far beyond the business prospects. Safeguarding citizens' integrity and privacy is a sine qua non for all; the US-EU Privacy Shield may eventually serve as a model also beyond the Atlantic. That way, we will truly have established a Shield for Privacy.

The Privacy Shield cannot stand alone if we want to unleash the promising business perspectives. This will also require substantial investment on many levels: business investment in human capital, technology and

infrastructure as well as public investment that can underpin the full transition to the knowledge society.

In times of heightened uncertainty where the repercussions of the financial crisis are only gradually getting behind us, the European Investment Plan may constitute an excellent catalyst for this much-needed extra investment. Lending from international banks, backed by guarantees from the EU budget and the European Investment Bank's own resources is already delivering this extra investment in Europe, thereby helping us to emerge as a structurally more competitive and resilient global business partner.

The Copenhagen Conference reaffirmed the huge potential from the business perspective, which suggests that this regulatory platform can deliver on our expectations for jobs and growth."


The first year of the European Investment Plan has confirmed that the strategy works: an additional 100 billion euros of investment has been approved, not least to SME's. That way, there is every prospect that the business opportunities unleashed by the Privacy Shield and backed and underpinned by the European Investment Plan are turning into real growth and jobs – for the benefit of businesses and consumers alike. 🇪🇺

Protection Reforms

Field: Opportunities Out of New Rules"

Value of BCCD's Business and Politics Forum

AT THE BCCD Business and Politics forums, companies can establish much closer links between today's political decisions and global business outcomes tomorrow. As a forward-looking Chamber, we know that key political decisions like negotiating an far reaching regulation could have serious implications for businesses, many of whom are our members with interests in the US and Europe. Our political independence gives us access to high-level speakers and policy makers that either companies or their trade associations would find difficult to reach. 🇵🇹



TRUST + CERTAINTY
=
OPPORTUNITY

Appendices

Appendix A – Authors:

Editor-in-Chief:

Mariano A. Davies

President & CEO, BCCD

Contact: mad@bccd.dk

Lead Author:

Deo Delaney

Head of Business Development,

EU and International Trade BCCD

Contact dd@bccd.dk

Contributing Authors:

Giovanni Buttarelli

European Data Protection Supervisor

John Frank

Vice President EU Government Affairs, Microsoft

Amit Bajaj

Head of North Europe, Tata Consultancy Services

Michael Vedsø

Acting Head of Office, EU Representation in Denmark

Maarten Meulenbelt

Partner, Sidley Austin LLP

Ulf Pehrsson

VP/Head of Global Government Relations, Ericsson

Jeppe Brogaard Clausen

Partner, NJORD Law Firm

Niels-Peter Kjølbye

Attorney, NJORD Law Firm

Research and Text Development:

James Gordon-Orr

Editing, Business Development Assistant, BCCD

Contact jgo@bccd.dk

Administration:

Thi Tham Thomasen

Office Administration Manager, BCCD

The British Chamber of Commerce in Denmark (BCCD) is a bilateral Chamber for British and Danish business people in Denmark and international business in general. The vision of the BCCD is to be a prominent promoter of business and culture between Britain, Denmark and the international business community.

Public Relations and Graphic Design:

Hill+Knowlton Strategies, Public Relations

Aubertin - Design & Graphics

Mønster Studios, Interior and Graphic Design

Appendix B – References:

All speakers and panelist (input for analyses)





THE NEW MINI CLUBMAN.

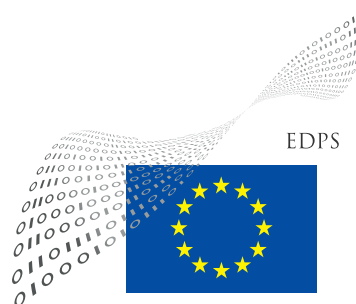
English heritage, German technology and Danish design. Read more at mini.dk



Editorial Contributors



European Commission
Representation in Denmark



Upcoming Events



7th Annual British Chamber Renewable Energy Conference

*“Reshaping the Feed-In Tariff System in Europe,
Who will pay the bill!”*

PriceWaterhouse Coopers Offices Hamburg
26th September 2016



Business Data Protection Authorities (DPA) Round Table

Danish Stock Exchange
September 2016

