# What are the main changes from the previous regulation?

 **“Legal Regulation and Professional Secrecy in the Age of PRISM”**

Interview with

*Dr. Péter Homoki, Chair of the CCBE Information Technology Law Committee*

The current regulation of Directive 95/46/EC has been shown to be inadequate, for one part thanks to changes in technology of data processing and the use of personal data, and for the other part due to the growing divergence in each country’s practise of implementation. To address these issues, the Commission decided to propose a new, comprehensive legal framework, that consists of a regulation (instead of the current directive) that encompasses almost all issues under within the scope of EU law (General Data Protection Regulation), except for the processing of personal data by authorities in relation to criminal offences and the execution of criminal penalties.[[1]](#footnote-1)

***Dr. Péter Homoki***

Providing a unified legal regime serves two main purposes: one is to strengthen a citizen's rights, and the other to provide a more harmonized regulatory background for businesses. Strengthened data protection rights can be viewed as a unified and effective right to be forgotten, a unified requirement of consent being an explicit one, the right to know what information is stored at a given data controller, and the new principle of data portability. Several measures, such as extending the powers of national data protection supervisory authorities, the accessible remedies and the widening of cooperation between such authorities complement such citizen rights.

Regarding the business side, considering the current differences between national regimes, a higher degree of harmonization could, in itself, be a big step forward – even considering the new regulatory burden being introduced. Nevertheless, more regulation does not necessarily mean better harmonization – even without any harmonization measure – it just certainly means more regulation and that judicial/authority practises could be even more divergent. So, for data controllers, the most promising step forward is the principle of a "single stop shop", i.e., that when a controller or processor is established in more than one member state, the supervisory authority located in the member state of the principal establishment of the controller or processor shall be solely competent.

# Do you think the self-regulation of the profession is under threat? What is the CCBE position on this?

The current proposals do keep certain issues open and are subject to the individual practise of a given data protection supervisory authority. Generally, such EU-wide extension in the scope of supervisory authorities necessarily constitutes a threat to self-regulatory bodies, like bars and law societies. But in the case of lawyers, this possible problem is exacerbated by the fact that we store data on behalf of our clients and the data subject – the person whose information is stored - may not necessarily be that of our client. It is part of our work and an integral part of our role as an independent profession to keep such a data without informing the person, and sometimes against the will of the data subject.

The CCBE's position paper on the Proposed Data Protection Reform[[2]](#footnote-2) was based on the better visibility of the legal privilege (professional secrecy) of lawyers under a data protection regime. It addressed, first, the issue of the “data subject's right to information and access”, which should not cover legally privileged information. Under the current wording of the proposed regulation, it is a risk that in, e.g., family law litigation, parties with a contrasting interest to that of the client could request a list of all personal data information possessed by the client’s lawyer.

The second issue relates to the power of supervisory authorities. The CCBE suggests the insertion of the possibility for member states to use the bars or law societies as data protection supervisory authorities (if they wish to act as such), because they are usually empowered to prohibit data control if necessary (i.e., effectively prohibit lawyers from processing personal data, and therefore from carrying out their professional duties), which would ensure that client data is protected to the same degree of care as the data of a lawyer. Furthermore, lawyers could send data protection breach notifications not to the general authority, but to their bars (should a particular member state decide to empower their national bar or law society with such a task).

# Do the same standards apply for protection of personal data for public and private parties?

Generally, yes, the proposed regulation should cover most of the control and processing of personal data by private and public bodies, but there are two very important exceptions. One is that issues "falling outside the scope of European Union law, in particular [those] concerning national security" are out of the scope of the proposed regulation. The other is that, as mentioned before, the control and processing of personal data by authorities in relation to criminal offences and the execution of criminal penalties is subject to a different regime that is based on a separate directive, not a regulation. The CCBE strongly regrets the choice of the European Commission to regulate data protection in the law enforcement area under an inferior level of protection as compared to the regulation.

It is not a good sign for businesses, in that what they will be required to comply with under the new integrated data protection regime proved too onerous for the law enforcement agencies of member states. This raises a question about properly balancing the impact of the reform package: is the new reform package really in the interest of businesses, if the cost for providing better protection to citizens is borne only by businesses? Is the amount of "red tape" that the Commission promised to cut in balance with the costs of complying with the new regulation?

# Why is the PRISM scandal and data mining by national governments important to us?

*PRISM, in brief: an employee of a private contractor of the National Security Agency (NSA) of the United States leaked classified information to journalists[[3]](#footnote-3). Among other issues, it revealed that internet and software giants such as Google, Microsoft and Facebook provided "direct access" to global data that they process and store, including Skype calls, video chats, e-mail, etc.*

For different people, PRISM tells a different story. For citizens, this is about trust in their own government – do they really use their powers according to law and their mandate, and are European countries able to protect their citizens from superpowers? For agencies, PRISM is more about how to prevent leaks from private contractors. For us average European lawyers, I think there are two issues here: one is about the question of legality and the other is about what we can do to help our clients.

It is very hard to say anything meaningful about PRISM as a legal issue. One can easily find disturbing, loosely related information such as: billions of bits of data intercepted by the NSA per year from certain EU countries and the UK's intelligence service (GCHQ*)* tapping transatlantic cables, etc. We, however, as lawyers cannot formulate a legal opinion about the legitimacy of methods used by the US and the cooperating agencies of EU members.

We do see that secret service agencies work in very similar ways on our side of the Atlantic: they have to work under certain safeguards (which are different country to country) and detailed rules are also not as visible here. This secrecy is necessary due to the nature of the game. Nonetheless, is this principle implemented in a proper way in practise? We do not know - either at national level or at the level of the EU.

I think that we, as lawyers, need to consider PRISM from this rather theoretical perspective. We also must know whether we have to try to better protect the legitimate interests of our clients. If yes, then we must examine which technical and regulatory tools would be the most useful in this scenario.

# What do you think we can learn from PRISM and what could be a way forward? Are the safeguards in the new proposed data protection directive sufficient?

Part of the solution might lie at the granularity of the rules regarding secret surveillance. If we take a look at its history, we can see that there has been a one-way tendency: over time, the practises of secret intelligence services are becoming more visible and, at the same time, more regulated. PRISM might be another milestone on this road. We already see the President of the US is setting up a review group and talks are commencing on a bilateral treaty between the US and Germany on restricting surveillance operations.

Subject to statutory safeguards, law enforcement and secret service agencies across all of Europe can and do have access to all citizen phone call logs, may wiretap them and read their mail or email. In spite of this, the exact conditions for such activities differ from country to country, e.g., access to the content of a communication might require reasonable suspicion and a judicial warrant in one country but not in another.

On the subject of secret surveillance, all we have in common are high-level principles and the case law of Article 8 of the European Convention on Human Rights (e.g., *Klass and others v. Germany, Leander v. Sweden or, Uzun v. Germany, Kopp v. Switzerland*.[[4]](#footnote-4))

This is clearly not enough to provide a minimum level of assurance for citizens at the EU level. That is exactly why the new proposed directive on data protection reform is very timely and a welcome change in this area. We must, however, emphasize that this latter instrument does not, at this moment, address the safeguards of secret surveillance and this directive will only apply to law enforcement – not to issues of national security.

As such, no matter what detailed rules we have, this will not necessarily change the question of trust by citizens. Information technology (IT) and telecommunications have become an integral part of everyday life and the technical capability of IT tools and available data has changed tremendously. If citizens now perceive the importance of secret surveillance powers very differently, it might be necessary to rebalance the actual practises of secret intelligence agencies and to define specific public guidelines for their work. Perhaps PRISM illustrates that the time has come for such a review.

# How can lawyers protect our clients from such acts?

We have to differentiate between protecting our clients from governmental access that we presume to be lawful, and protection from access without such a legal base.

We are required to protect the confidentiality of our clients' data due to both lawyer specific legislation (professional secrecy) and, as data processors, to data protection requirements. But, can we as lawyers, as a constituent part of the justice system of a country, aid our clients in shielding their information from surveillance that we have to presume to be lawful? Can we deliberately protect our clients' legitimate interest against the legitimate interests of national security? Is there a law preventing lawyers from trying to do this? Would such a law constitute disproportionate interference with the professional privilege of lawyers?

Regardless of any inquiry outcome, whether the United States of America, the United Kingdom, Germany, etc. all acted within their constitutional duty (if any), we as lawyers have to take into account that it is no longer just a rumour that secret surveillance agencies have access to our email and telephone correspondence with our clients, or to the files we store at those internet giants who have a backdoor agreement with NSA.

I can imagine that in international tendering processes, some clients could be afraid of secret intelligence services helping their own national businesses under the pretext of national security, and no legal counsel could dispel such a fear.

Therefore, as lawyers, it might be necessary to keep in mind certain principles. Cost-wise, it is very different for an agency to write a letter or email to a service provider to ask for specific data on certain people, rather than to be able to pre-filter huge amounts of data via keywords and to further process any snippets that might be interesting according to precise data requests - even if the legal background was the same in both cases. We need to take into consideration that automated access to emails and other written conversations and their automated processing is much cheaper than transcribing discussions over the telephone.

We at the CCBE IT Law Committee have carried out several internal surveys. The results suggest that the strongest legal protection offered to a client's files is in a lawyer's office (which requires a judicial warrant for a search). When the lawyer stores this information at a third party location - be it an international cloud service provider or a simple data centre next door - this judicial warrant protection is no longer effective. Of course, working only in "lawyer premises", is usually not in most clients' expectations, nor in current IT products. On the other hand, we cannot resort to using pigeons and couriers.

It would be, nevertheless, wise to support the spread of more secure communications over the internet than the current unencrypted email – at least between lawyers and to provide such options to our clients. However, we also have to acknowledge the huge costs of such lawyer-specific approaches, of maintaining these in the long term and the risks of inter-operability.

We cannot expect our clients to spend money, change their IT or encrypt every outgoing email just to safely communicate with lawyers. Moreover, we also cannot expect to have any effect regarding the US as the backbone of the internet or on US-based companies who are the market leaders of the most popular services, and in the efforts of such companies to be in compliance with their own national requirements, regardless of whether we, in the EU, agree with these principles or not.

# What can the bars do in helping the lawyers?

Public data cloud aggregation websites have already shown a great deal of problematic issues for lawyers to consider[[5]](#footnote-5). A lawyer will most probably need at least an informed consent from their client to use a cloud to store client data. A lawyer will have to check whether required safeguards are present in the service offering. And last, but not least, we have to trust that what the service provider writes in the contract is, and remains, true.

A question has been raised about whether it would be in any way better to build and maintain a national or an EU-wide “community cloud for lawyers”, with a guarantee of no backdoor. One problem is the cost. For mass users, such as lawyers, cloud computing is more about economies of scale, not about easier configuration, and only a few bars are large enough to make this a viable solution. An EU-wide approach could be more meaningful, but that does not mean that this is the right approach. If one of the governments physically hosting the site adopts an obligation to grant backdoor access, this whole exercise would become futile.

# Does professional secrecy even exist anymore in this framework?

At the level of the EU, similar to the lack of regulation of safeguards against secret surveillance, there is no minimum level of protection for legal privilege. At this level, all we have is *AM & S Europe Limited v Commission of the European Communities*[[6]](#footnote-6), and The Charter of Fundamental Rights of the European Union[[7]](#footnote-7), which builds upon Article 8 of the European Convention on Human Rights[[8]](#footnote-8) and invaluable related case law. Respecting the right of professional secrecy is as much an essential part of the rule of law as the existence of an independent legal profession. If there is a general lack of trust about the surveillance powers of the state, professional secrecy will also suffer. If the general rules on the practises of secret surveillance are revised due to technological changes, any new rules should also take into account potential changes in how lawyers work.

If lawyers have no choice in keeping client data in-house and on premises because new computing platforms presume working from the cloud, than client data will have to be protected by law accordingly as well. In this context, it should not be lawful for agencies to have access to client data from a lawyer's account without exactly the same warrants that are otherwise necessary for accessing paper-based files.

# What role will the bars play according to the current European projects?

Self-regulation capabilities are at the essence of the independence of the legal profession. As more e-government initiatives take place at the EU level (e.g., e-CODEX), it becomes indispensable for bars to represent the interests of their lawyers at this level as well. Although lawyers work under very different legal regimes and under vastly different organisations, we have a common interest in participating as early as possible in any new e-government initiatives and projects.

We cannot expect governments and bodies of the EU to speak for us, to develop solutions that are not only accessible to citizens, but that also cater to the special needs of lawyers. Even though the usefulness of an independent legal profession is never questioned, we must actively participate in e-government solutions in order to not be treated in the same manner as the clients that we represent. Without lawyer-specific input, implemented e-government solutions will only be tailored to individual citizens, and therefore lawyers will not be technically able to realize their full capabilities. We will not be able to facilitate the interaction between government and citizens (business), and that is, in itself, a very large long-term risk.

The risk is not that e-government services or IT would displace lawyers as a whole (although there are considerable areas where this will be an issue), but that the importance and capabilities of our profession will be decreased, with clients simultaneously receiving a lower level of service.

This is why it is important for the bars to not only react at the national level of e-government services, but likewise at the EU level as well. It is significantly easier to find a working solution at the CCBE that is good for both lawyers in Slovakia and in the UK, than to find a common platform at national levels, which are lumped together with the problems of courts, ministries and citizens. Our experiences with e-CODEX and Find-A-Lawyer have clearly shown that the CCBE's opinion is duly taken into account at the EU level.

1. Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. [↑](#footnote-ref-1)
2. Position on the Proposed Data Protection Reform Package COM(2012) 11 and COM(2012) 10: <http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/07092012_EN_CCBE_Pos1_1361196843.pdf> [↑](#footnote-ref-2)
3. See the PRISM timeline: <http://www.guardian.co.uk/world/2013/jun/23/edward-snowden-nsa-files-timeline> [↑](#footnote-ref-3)
4. And of course, similar provisions of the Charter of Fundamental Rights of the European Union, and Article 16 of Treaty on the Functioning of the European Union, and declarations 20-21 of Annex II thereof – but these could not be considered as providing more details on this subject compared to the case law of ECHR Article 8. [↑](#footnote-ref-4)
5. See the "CCBE Guidelines on the Use of Cloud Computing Services by Lawyers": <http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/07092012_EN_CCBE_gui1_1347539443.pdf> [↑](#footnote-ref-5)
6. Case 155/79 *AM & S Europe Limited v Commission of the European Communities* [1982]: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61979CJ0155:EN:HTML> [↑](#footnote-ref-6)
7. <http://ec.europa.eu/justice/fundamental-rights/charter/> [↑](#footnote-ref-7)
8. <http://www.echr.coe.int/Documents/Convention_ENG.pdf> [↑](#footnote-ref-8)