EUROPEAN
POLICYBRIEF

INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES (IRISS)

POLICY BRIEF[1]

Recommendations to the Council of the EU and the European Parliament on access rights, in the context of the European data protection reform

31 January 2015

PREAMBLE

The right of access to personal data is a central feature of European data protection law. It is, arguably, the most important of the so-called "ARCO" data protection rights (access, rectification, cancellation, opposition) because, if one cannot discover what is held about oneself, it is not possible to exercise the remainder of these rights. Furthermore, the right of access to personal data is essential to uncovering illegal and illegitimate surveillance practices[2].

Ten European universities and research centres have recently undertaken research on the exercise of access rights in Europe within the framework of the project IRISS, Increasing Resilience in Surveillance Societies. Our study[3] was conducted across ten European countries[4] and investigated over 300 public and private organisations, including responses to 184 subject access requests submitted by researchers.[5] The findings have highlighted important problems and difficulties in the exercisability of access rights from the perspective of the data subject. Obstacles to the exercise of access rights are exacerbated by the existing European data protection legal framework, the reform of which is underway.[6] We therefore urge the Council and the European Parliament (EP) to consider carefully the recommendations emerging from this research, particularly in the context of the proposed General Data Protection Regulation and Directive.

FINDINGS

The IRISS research found that the spirit of the European Data Protection Directive (Directive 95/46/EC) has frequently been blunted as it has been transposed into national legal frameworks, and sometimes further undermined by national case law. Citizens, in their role as data subjects, encounter a wide range of legitimate but not always convincing and straightforward restrictions in their attempts to exercise their rights. These restrictions are further abetted by illegitimate actions enacted through various types of access denial practiced by data controllers or their representatives. The main findings can be summarised as follows.

- Owing to inconsistent national implementation of data protection legislation in Europe, data subjects in different countries are subject to different frameworks in the context of exercising their right of access. This includes differing rules on: the cost of submitting a request; the requirement of including identification documents; the legally-stipulated timeline by which data controllers must respond to a request; the possibility of getting direct and/or indirect access to personal data contained in police files; and the cost of redress mechanisms involving different Data Protection Authorities at national levels.

- Accessing personal data was at times restricted by the necessity to provide a "motivated reason" for the request, which is a legal provision in some European countries.[7] The need to justify an access request as a precondition of access to personal data goes against European data protection law. Moreover, there is little or no clarification of the criteria of validity for such reasons, causing uncertainty and ambiguity when attempting to exercise one's access rights in practice.

- In one-fifth (20%) of cases, information provided by organisations was of such poor quality that it was not possible to identify a competent officer within the data controller's organisation in order to submit an access request.

- A similar outcome was reached with regard to the 49 CCTV systems we researched: although identifying the controller of CCTV data is essential for making a subject access request, a fifth (20%) of all CCTV operators failed to display any CCTV signage.

- Among those CCTV operators who did display signage, only one-third (33%) included data controller information on the signage.

- Four-in-ten subject (43%) access requests submitted in the research did not result in personal data being disclosed or in data subjects receiving a legitimate reason for the failure to disclose their personal data.

- In over half of all cases (56%), no adequate or legally compliant response was received concerning third-party data sharing.

- In over two-thirds of cases (71%), requests for information about automated decision-making processes were either not answered or not answered in a legally compliant manner.

- Holding or acknowledgement letters were received in only one-third (34%) of cases, which meant that data subjects had no idea whether the requests were being dealt with or simply ignored.

- 15% of access requests submitted to data controllers were met with silence.

- Data controllers were generally reluctant to disclose any information about their data sharing protocols, and even when pressed, only revealed generic lists of those with whom they shared personal data.

- Data controllers were generally unable to say when and how automated decision-making processes were used when questioned about them.

- There is a lack of clarity as to which national legislation, if any, international companies are subject to, with regard to access rights.

- More than one-fifth (21%) of all requests for their personal data needed to be referred by the IRISS requesters to their respective national Data Protection Authorities due to the unsatisfactory conduct of data controllers.[8]

The multitude of restrictive practices evidenced in this research means that data subjects often have to work extremely hard to make progress in exercising their right of access. To succeed, they must show persistence, confidence and resilience in the face of a series of access-denying tactics, during which their access requests may be regarded as illegitimate, severely delayed or simply ignored altogether. This situation is often compounded by an endemic lack of awareness among organisations about data protection requirements and specifically about the right of access. As such, organisations' representatives repeatedly reacted with surprise and puzzlement to requests, explaining that they had never before received such queries. A vicious circle therefore emerges, in which organisations fail to inform citizens of their rights or how to exercise them. As a result, for those citizens who have little or no prior knowledge about privacy and data protection issues, the right of access is either unknown, denied or unusable. Owing to the lack of subject

access-related queries received from the public, organisations then have little motivation to inform or train their staff in matters of privacy and data protection.

POLICY RECOMMENDATIONS

In light of the findings above, a number of policy recommendations are outlined here. Following discussions with representatives of six European Data Protection Authorities, these recommendations are presented with a view to informing the ongoing European data protection reform, and we encourage the Council and the European Parliament to consider these carefully in drafting the new legal framework.

- General Data Protection Regulation (GDPR): We welcome the use of a Regulation rather than a Directive to replace Directive 95/46/EC as a general data protection law instrument. The choice of a Regulation, applicable in all areas of data protection with the exception of the police, will lead to greater harmonisation between different countries with regard to subject access rights.

- General Data Protection Directive (GDPD): We welcome the use of a Directive to harmonise data protection rules with regard to processing of data by police forces in an area that was until now beyond the reach of EU law.

- The content of access rights in both EU instruments should be further clarified: The right to obtain a copy of one's own data or the documents containing such data should be the main rule, not only a specific rule in case of electronic processing, as it is now in Art. 15.2a GDPR. Otherwise the wording of Art. 15.2 GDPR would allow data controllers to restrict access rights only to giving secondary information about the data. It should be the controller's obligation to provide the necessary technical and organisational conditions for facilitating subject access and providing copies of the data and documents, in particular in the case of CCTV recordings.

- Harmonisation of procedures and deadlines: The GDPR and GDPD will harmonise procedures and deadlines for exercising access rights. Art. 12.2 GDPR goes in this direction and we welcome this provision. However, clear rules on procedures and deadlines for exercising access rights do not emerge from the proposed GDPD. Moreover, the GDPD does not clarify if and in which cases access to personal data should be indirect. From a human rights perspective, direct access should be the rule and only selective use should be made of the indirect access mechanism.

- Data Protection Officers (DPOs): We welcome the proposed obligation to appoint DPOs established at Art. 35 GDPR and Art. 30 GDPD, because DPOs could help to improve data controllers' procedures for fulfilling subject access requests Moreover, we also welcome the European Parliament's (EP) proposal to set this obligation on enterprises which process sensitive data, location data or data on children or employees in large-scale filing systems. However, we would not recommend setting minimum criteria for the appointment of DPOs, such as the number of data subjects whose data is processed, as is currently outlined at Art. 35.1(b) of the EP's consolidated version of the new Regulation. Instead, we recommend that all organisations processing personal data have, as a minimum standard, a nominated officer who is fully trained in data protection matters and is able to process and respond to subject access requests.[9]

- Privacy policies: If data subjects are to be empowered to exercise their rights, organisations must clearly describe their subject access procedures and policies and provide explicit protocols for submitting an access request. We welcome provisions of the GDPR and GDPD that go in this direction.[10]

- Third-party data sharing: The expression "recipients *or* categories of recipients" of Art. 15.1 (c) GDPR and Art. 12.1 (c) GDPD should be replaced by the more demanding expression, "recipients *and* categories of recipients" (italics added). The European Parliament's consolidated version of the new Regulation refers to "recipients" only at its Art. 15.1 (c), thus excluding information on the categories of recipients. In our view, this amendment would give data subjects the possibility of having exact information about third-party data sharing. However, the provision "recipients *and* categories of recipients" would add further clarity on this point. This is particularly so because declaring the categories of recipients (for instance in online privacy statements) would enable data subjects to know how their data may be used and shared before they actually provide controllers with their data.

- Profiling: We support the amendments proposed by the EP to the GDPR concerning profiling. In particular, we support the provision established at Art. 20.5 of the EP's consolidated text, which will include "human assessment" in automated processing decisions.[11] A similar provision can be found in the consolidated version of the GDPR proposed by the Council.[12] We also welcome the obligation on the data controller to disclose "meaningful information about the logic involved in any automated processing".[13] However, the proposed Art. 20 GDPR does not clarify whether or not there is an obligation on data controllers to disclose information about the algorithm involved in profiling practices. We suggest clarification on this point.

- Motivated requests: No obligation to motivate (give a reason for) access requests is foreseen in the proposed GDPR and GDPD. However, we invite the Council and the EP to address this issue, explicitly establishing that in no case may the data controller require motivation from the data subject as a precondition of access.

- Transnational companies: Insofar as it affects subject access rights, the lack of clarity about jurisdiction should be addressed.

Conclusion

The recommendations made in this Policy Brief are based on extensive research conducted by the IRISS project. We urge the Council and the European Parliament to consider this submission carefully as the reform process continues.

Addendum on the Role of DPAs

Data Protection Authorities (DPAs) have a crucial role to play with regard to subject access rights. Our research findings suggest that DPAs can ameliorate the unsatisfactory situation outlined above and that DPAs can help to make the application of the (existing or forthcoming) legal rules easier. The following recommendations are made in order to strengthen DPAs in this role insofar as they may not already be performing these activities:

- DPAs should actively promote information rights to citizens and give some consideration of how training and awareness-raising could be delivered.

- DPAs should provide standard model templates for data subjects to use in order to submit an access request.[14] In conjunction with relevant stakeholders such as consumer-rights and labour organisations, they should also promote standard templates in specific sectoral contexts.[15]

- DPAs should provide detailed guidance to data controllers in how to respond to access requests, including examples of best practice,[16] and give some consideration to how specific training could be delivered.[17]

- DPAs should also provide detailed guidance to data subjects on how to exercise their rights.

- DPAs should ensure that a clear, unambiguous and affordable complaints procedure is always available to data subjects who believe that data controllers have not fulfilled their duties.

- DPAs should have the power of audit and inspection as this would go some way to redress the asymmetry of power experienced between data subjects and data controllers.

- DPAs should proactively audit public and private sector organisations' web sites and other channels of communication to see whether all relevant information is available to citizens to make a successful access request.[18]

- Lastly, DPAs should use their European networks (Article 29 Working Party and others) further to harmonise the legal and operational framework on access rights.

ENDNOTES

[1] This policy brief was drafted by Professor Clive Norris, Dr Xavier L'Hoiry, Antonella Galetta, Professor Paul De Hert, Dr Ivan Szekely and Professor Charles Raab for and on behalf of all the members of the IRISS consortium. We are particularly grateful to the senior officials of the Austrian, Belgian, Hungarian, Italian, Norwegian, and United Kingdom Data Protection Authorities whose comments and reflections on our research have helped shape our recommendations

[2] In particular see the findings of IRISS Work Package 3, entitled "Surveillance impact on open and democratic societies" led by Professor Kirstie Ball (Open University, UK). This study documents the lack of transparency and accountability of surveillance regimes that citizens can be subject to. The study can be accessed at: http://irissproject.eu/?page_id=9

[3] The study was developed within IRISS Work Package 5, entitled "Exercising democratic rights in surveillance regimes", led by Professor Clive Norris and Dr Xavier L'Hoiry (University of Sheffield, UK) in collaboration with: Antonella Galetta (Vrije Universitiet Brussel, Belgium); Professor Paul De Hert (Vrije Universitiet Brussel, Belgium); Dr Ivan Szekely (Eotvos Karoly Institute, Hungary); Beatrix Vissy (Eotvos Karoly Institute, Hungary); Dr Rocco Bellanova (Peace Research Institute Oslo, Norway); Professor J. Peter Burgess (Peace Research Institute Oslo, Norway); Maral Mirshahi (Peace Research Institute Oslo, Norway); Stine Bergersen (Peace Research Institute Oslo, Norway); Marit Moe-Pryce (Peace Research Institute Oslo, Norway); Jaro Sterbik-Lamina (Institute of Technology Assessment, Austria); Stefan Birngruber (Institute of Technology Assessment, Austria); Dr Chiara Fonio (Universita Cattolica del Sacro Cuore, Italy); Alessia Ceresa (Universita Cattolica del Sacro Cuore, Italy); Professor Marco Lombardi (Universita Cattolica del Sacro Cuore, Italy); Dr Gemma Galdon Clavell (Universitat de Barcelona); Dr Liliana Arroyo Moliner (Universitat de Barcelona); Dr Erik Lastic (Univerzita Komenskeho v Bratislave, Slovakia); Roger von Laufenberg (Institut fur Rechts und Krimialsoziologie, Austria); Professor Nils Zurawski (Universitat Hamburg, Germany); Dr Keith Spiller (Open University); Professor Charles Raab (University of Edinburgh, UK).

[4] This research was conducted in the following countries: Austria, Belgium, Germany, Hungary, Italy, Luxembourg, Norway, Slovakia, Spain and the United Kingdom.

[5] Full Deliverable and all appendices available at: http://irissproject.eu/?page_id=9

[6] The reform process will result in the European General Data Protection Regulation (GDPR) and General Data Protection Directive (GDPD).

[7] Such as when requesting CCTV footage in Belgium and Luxembourg.

[8] Many more complaints could have been submitted but finite resources in the research meant that researchers only submitted a selection of cases in which it was deemed that data controllers had displayed particularly restrictive practices and behaviour.

[9] This does *not* mean that all data controllers should employ a dedicated Data Protection Officer who deals exclusively with data protection matters. Rather, this may simply be an existing member of staff with other duties and responsibilities who has received sufficient training to enable them to process and respond to requests in a legally compliant manner.

[10] In particular, Art. 11 and 14 GDPR and Art. 10 and 11 GDPD.

[11] According to Art. 20.5 proposed by the European Parliament, "Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment. The suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2 shall include the right to obtain human assessment and an explanation of the decision reached after such assessment".

[12] Art. 20.1b of the proposed text.

[13] See Art. 15.1 (ha) of the EP's consolidated version of the GDPR

[14] See for example the templates provided by the Italian DPA, available at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089924.

[15] This may include specifically the financial sector. Another strand of the research conducted within IRISS evidenced considerable uncertainty for data subjects in the area of credit scoring, where greater transparency would be beneficial. This could, in part, be achieved via the right of access to personal data. For further information, see http://irissproject.eu/?page_id=9

[16] See for example the Information Commissioner's Office (2012) "Draft Subject Access Code of Conduct" http://www.ico.gov.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/draft_subject_access_cop_for_consultation.ashx

[17] See for example the detailed guidance provided in the IRISS deliverable concerning how to respond to access requests and the importance of providing data protection awareness training to all staff within organisations. This is available at http://irissproject.eu/?page_id=9

[18] It may be the case that DPAs do not have the resources to undertake such work. Instead, DPAs could work collaboratively with non-governmental organisations (NGOs) to facilitate their attempts to undertake such tasks.

PROJECT IDENTITY

PROJECT NAME

Increasing Resilience in Surveillance Societies (IRISS)

CO-ORDINATOR

Reinhard Kreissl, Institute for the Sociology of Law and Criminology (IRKS) / Vienna Centre for Societal Security (VICESSE), Vienna, Austria.
Reinhard.Kreissl@vicesse.eu

CONSORTIUM

Comenius University (COMENIUS, Slovakia
Eotvos Karoly Policy Institute (EKINT), Hungary
Fundació per a la Universitat Oberta de Catalunya (UOC), Spain
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Germany
Institute for the Sociology of Law and Criminology (IRKS), Austria
Institute of Technology Assessment (OeAW-ITA), Austria
Open University (OU), United Kingdom
Peace Research Institute Oslo (PRIO), Norway
Trilateral Research & Consulting (TRI), United Kingdom
Universita Cattlocia des Sacro Cuore (UCSC), Italy
Universitat de Barcelona (UB), Spain
Universität der Bundeswehr (UNIBW), Germany
University of Edinburgh (UEdin), United Kingdom
Universität Hamburg (UH), Germany
University of Sheffield (USFD), United Kingdom
University of Stirling (STIR), United Kingdom
Vrjie Universiteit Brussel (VUB), Belgium

FUNDING SCHEME

FP7 Framework Programme for research of the European Union
SSH.2011.5.1-2 Surveillance and the challenges for democracy and an open society

DURATION

February 2012 – January 2015 (36 months)

BUDGET

EU contribution: €2,596.770.

WEBSITE

Irissproject.eu

FOR MORE INFORMATION

Please contact:

Professor Clive Norris, Department of Sociological Studies, University of Sheffield, Sheffield, UK, S11 2TU; email - c.norris@sheffield.ac.uk

Professor Paul De Hert, Department of Interdisciplinary Studies of Law (Metajuridica), Faculty of Law and Criminology, Vrije Universiteit Brussel (VUB), Pleinlaan, 2, 1050 Belgium; email - paul.de.hert@uvt.nl