Die Landesbeauftragte
für den Datenschutz und
für das Recht auf Akteneinsicht

LAND BRANDENBURG
LDA
Schutz der
• Persönlichkeitsrechte
• Informationsfreiheit

Internationales Symposium Informationsfreiheit und Datenschutz

Datenschutz und Informationsfreiheit – Widerspruch oder Ergänzung?

28. September 2017

Dokumentation

Akteneinsicht und Informationszugang
Potsdamer Materialien
Band 10

LAND BRANDENBURG

LDA

Schutz der
• Persönlichkeitsrechte
• Informationsfreiheit

Internationales Symposium
International Symposium

Datenschutz und Informationsfreiheit – Widerspruch oder Ergänzung?

Data Protection and Freedom of Information – Contradiction or Complement?

28. September 2017 in Potsdam

Veranstaltung der
Landesbeauftragten für den Datenschutz
und für das Recht auf Akteneinsicht

Dokumentation

Impressum

Herausgeber: Die Landesbeauftragte für den Datenschutz und
für das Recht auf Akteneinsicht Brandenburg
Stahnsdorfer Damm 77, Haus 2
14532 Kleinmachnow

Telefon: +49 33203 356-0
Fax: +49 33203 356-49

E-Mail: Poststelle@LDA.Brandenburg.de
Internet: http://www.lda.brandenburg.de

Fingerprint: E899 5780 7F65 F282 8CAC C504 37F3 83FE 0844 834D

Druck: Brandenburgische Universitätsdruckerei und
Verlagsgesellschaft Potsdam mbh

Dezember 2017

In der Reihe „Potsdamer Materialien zu Akteneinsicht und Informationszugang“ sind bisher erschienen:

Band 1: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz; 25./26. Oktober 1999

Band 2: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz in der erweiterten Europäischen Union; 8./9. Oktober 2001

Band 3: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz – Transparenz und E-Government in Mittel und Osteuropa; 10./11. November 2003

Band 4: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz – Informationsfreiheit in Deutschland und Europa; 28./29. September 2005

Band 5: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz – Öffentliche Daten auf dem privaten Markt – neue Regelungen zur Weiterverwendung öffentlicher Informationen; 4./5. Juni 2007

Band 6: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz – Zugang zu Umweltinformationen – Informationsfreiheit für den Umweltschutz?; 18./19. Juni 2009

Band 7: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz – Verbraucherinformationen – Marktregulierung durch Transparenz?; 30./31. Mai 2011

Band 8: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz – Open Data – Ergänzung oder Einschränkung der Informationsfreiheit?; 27. Mai 2013

Band 9: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz – Informationsfreiheit und die Wirtschaft – zwei Welten?; 8. Juni 2015

Band 10: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz – Datenschutz und Informationsfreiheit – Widerspruch oder Ergänzung?; 28. September 2017

Inhalt

Dagmar Hartge
Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht Brandenburg

Eröffnung

Sehr geehrte Frau Abgeordnete,
sehr geehrter Herr Prof. Dr. Günther,
liebe Kolleginnen und Kollegen,
sehr geehrte Gäste unseres Symposiums,

ich freue mich, Sie am heutigen Internationalen Tag der Informationsfreiheit, dem „Right to Know Day“, zu unserem Internationalen Symposium in Potsdam begrüßen zu können. Dieser Tag wird bereits seit dem Jahr 2002 am heutigen Tag weltweit begangen. Was also lag näher, als unser Symposium am heutigen Tag zu veranstalten und es dem Thema Informationsfreiheit in einem europäischen Kontext zu widmen.

Der „Right to Know Day“ – ich finde die englische Bezeichnung noch treffender als die deutsche Bezeichnung – erinnert uns daran, dass das Recht zu Wissen bis heute nicht für alle Bürgerinnen und Bürger selbstverständlich geworden ist. Nicht zuletzt in Deutschland tun sich noch immer einzelne Bundesländer ausgesprochen schwer damit, Informationsfreiheit in ihren Ländern gesetzlich zu verankern.

Dies ist in Brandenburg anders. In Brandenburg sind Datenschutz und Informationsfreiheit in der Landesverfassung geregelte Grundrechte der Bürgerinnen und Bürger. Beide Rechte wurden Anfang der 90er Jahre vom Verfassungsgeber als wesentlich für eine funktionierende Gesellschaft angesehen. Die Landesverfassung und auch das Brandenburgische Datenschutzgesetz haben in diesem Jahr bereits ihren 25. Geburtstag gefeiert. Das brandenburgische Akteneinsichts- und Informationszugangsgesetz dagegen wurde als erstes Informationsfreiheitsgesetz der Bundesrepublik Deutschland erst sechs Jahre später, nämlich im Jahr 1998, vom brandenburgischen Parlament verabschiedet. Seitdem haben die Bürgerinnen und Bürger unseres Landes einen einklagbaren Anspruch auch auf Akteneinsicht im Sinne der Informationsfreiheit.

Gut zwanzig Jahre Informationsfreiheit sind nur ein kurzer Zeitraum, wenn man einen Blick auf die skandinavischen Länder wirft. Dort existiert

dieses „Right to Know“ mit dem damaligen Gesetz über die Pressefreiheit bereits seit 1766. Dies ist wahrlich ein Unterschied.

Nach der nun mehr als zwanzig Jahre bestehenden Koexistenz von Datenschutz und Informationsfreiheit in Brandenburg hat sich mir die Frage gestellt, wie es nach dieser Zeit des Nebeneinanders der Gesetze und damit beider Ansprüche eigentlich aussieht mit dem Zusammenspiel der Ansprüche? Passen das Recht auf informationelle Selbstbestimmung des Einzelnen als Recht auf Schutz seiner personenbezogenen Daten und das Recht auf Einsicht in Akten öffentlicher Stellen wirklich immer zusammen? Ist das nicht vielleicht ein Widerspruch in sich? Akten öffentlicher Stellen enthalten sehr häufig auch personenbezogene Daten, die mehr oder weniger sensibel sind. Man denke nur an personenbezogene Daten im Gesundheitsbereich oder auch Daten aus Polizeilichen Akten und Dateien. Muss es nicht zwangsläufig zu Konflikten kommen, wenn jemand Akteneinsicht in einen Verwaltungsvorgang begehrt, der auch personenbezogene oder personenbeziehbare Daten enthält? Ist es nicht wie bei einem Kräftemessen ein regelmäßiges Ziehen in die jeweils eigene Richtung? Wer gewinnt bei diesen Fällen eigentlich? Können beide Seiten Sieger sein? Schließen sich der Schutz der personenbezogenen Daten vor unbefugter Offenlegung und die mit der Informationsfreiheit verbundene Transparenz am Ende nicht doch aus? Sie sehen: Fragen über Fragen.

Auch die Frage des Zusammenpassens beider Rechte in einer Kontrollbehörde bewegt die Gemüter immer wieder, besonders dann, wenn erstmals ein Gesetz zur Regelung der Informationsfreiheit verabschiedet wird. Oft wird diese Frage auch danach immer wieder aufgeworfen. Kann eine gemeinsame Kontrollbehörde wirklich beiden Rechten gerecht werden? Gerade bei zwei so unterschiedlich großen Bereichen ist diese Frage ja durchaus berechtigt. Können Kollisionen innerhalb einer zuständigen Behörde vernünftig gelöst werden oder vielleicht sogar besser? Weil sich all diese Fragen einfach stellen, ist ein Blick auf unterschiedliche Modelle der „Aufsicht.“ in der Praxis immer hilfreich. Unser Symposium bietet hierfür eine gute Möglichkeit.

Ich freue mich, dass ich für unser europäisches Symposium so viele engagierte Referentinnen und Referenten für die verschiedenen Fragestellungen und Blickwinkel gewinnen konnte. Wie es schon fast Tradition geworden ist, bereichert auch in diesem Jahr wieder eine europäische Institution, dieses Mal eine Vertreterin des Europäischen Datenschutzbeauftragten, unsere Veranstaltung. Viele spannende Einzelbeispiele zu den grundsätzlichen Fragestellungen des Zusammenpassens wie auch

praktische Beispiele, die aufzeigen, wie das Zusammenspiel funktioniert, illustrieren die aufgeworfene Fragestellung des Symposiums. Wie immer haben wir auch die Wissenschaft mit einem Vortrag in unseren Strauß an Einblicken eingebunden. Mit Referentinnen und Referenten aus Brüssel, Kroatien, der Ukraine, Albanien, Luxemburg und Deutschland ist dieses Symposium tatsächlich international. Dass dies möglich ist, erfüllt mich immer wieder mit großer Freude. Nicht zuletzt deshalb, weil die Vorträge immer wieder zeigen, dass gute Ideen überall gedeihen können und der Erfahrungsaustausch für uns alle ein großer Gewinn ist.

Datenschutz und Informationsfreiheit sind zwar jeder für sich begrifflich sehr sperrig und sehr abstrakt, doch beide Rechte sind eng mit dem Ziel demokratischer Teilhabe verbunden. Leider wird fast immer nur das Datenschutzrecht in der Öffentlichkeit diskutiert und bemerkt; zu selten findet das Recht auf Informationsfreiheit den Weg in das öffentliche Bewusstsein.

Deshalb ist mir die Möglichkeit, die dieses Symposiums eröffnet, besonders wichtig, heute mit Ihnen gemeinsam der Frage nachzugehen, wie diese beiden Rechte sich eigentlich zueinander verhalten. Welche Erfahrungen haben andere europäische Staaten mit den beiden Rechten gemacht? Sind sie ein gutes Team oder sind sie sich bekämpfende Gegner, die gar nicht zueinander kommen können. Die Antwort auf die Ausgangsfrage nach Widerspruch oder Ergänzung wird sich am Ende jeder selber geben müssen.

Das Grußwort zu unserem Symposium wird zu meiner Freude heute der Präsident der Potsdamer Universität Herr Prof. Dr. Günther sprechen. Als Vertreter der Wissenschaft in Potsdam hat er seinen ganz eigenen Blick auf das Verhältnis der beiden Rechte. Sehr geehrter Herr Prof. Dr. Günther, ich freue mich auf Ihr Grußwort und anschließend spannende Vorträge und ebenso spannende Diskussionen.

Data protection and access to public documents in the EU

Anna Buchta
EDPS

International Symposium "Data Protection and Freedom of Information – Contradiction or Complement?"
Potsdam, Germany
28 September 2017

European Data Protection Supervisor

1. **Supervise** data processing done by EU institutions and bodies;
2. **Advise** the EU legislator and appear before the EU courts;
3. **Monitor** new technologies with an impact on privacy;
4. **Cooperate** with other supervisory data protection authorities.

Data protection and access to documents in EU law

1. EU legal framework for personal data protection and transparency/access to documents
2. How is the balancing done? (CJEU case law)
3. Examples from EDPS practice
4. Pending issues & utlook

EU primary law: data protection

Article 7 CFREU
Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 CFREU
Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

EU primary law: transparency

Article 15 TFEU

1. In order to promote good governance and ensure the participation of civil society, the Union's institutions, bodies, offices and agencies shall conduct their work as openly as possible.
(...)
3. Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, shall have a right of access to documents of the Union institutions, bodies, offices and agencies, whatever their medium (...)

Article 42 CFREU

Right of access to documents

Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, has a right of access to documents of the institutions, bodies, offices and agencies of the Union, whatever their medium.

The European Code of Good Administrative Behaviour

The public service principles that should guide EU civil servants:

Transparency:

"Civil servants should be willing to explain their activities and to give reasons for their actions.

They should keep proper records and welcome public scrutiny of their conduct, including their compliance with these public service principles."

Legal framework for EU institutions: data protection

- Regulation (EC) No 45/2001 on data protection
  - very close in substance to Directive 95/46/EC incl. principles, data subjects' rights, independent supervision...
  - particular features include:
    - obligation to appoint a DPO
    - "transfers" to recipients subject to general data protection law are subject to a necessity test + no prejudice to legitimate interests (Article 8)

Legal framework for EU institutions: access to documents

- Regulation (EC) No 1049/2001 on public access to official documents
  - Any natural or legal person
  - No obligation to give reasons for the request
  - All documents drawn up or received in all areas of activity
  - Document: any content whatever its medium
  - No privileged access (ex: MEPs have the same right as members of the public)
  - “Absolute” exception in Article 4(1)(b): privacy and integrity of the individual

The balancing act

- ***Bavarian Lager*** (C-28/08 P): both regulations must be applied simultaneously and in full
  - Conditions for disclosure of personal data:

    (1) express and legitimate justification, convincing argument to demonstrate necessity;

    (2) the institution must determine whether there is reason to assume that data subjects legitimate interests might be prejudiced; if there is no such reason, the transfer must be made;

    (3) if there is a reason to assume that legitimate interests of the individual concerned might be prejudiced, the institution must weigh up the various competing interests in order to decide on the request for access.

How to establish necessity?

- ***Dennekamp II*** (T-115/13)
  - high threshold for necessity test: disclosure must be the most appropriate of the possible measures and proportionate;
  - express and legitimate reasons needed, e.g. conflict of interest (defined in financial terms)
- ***ClientEarth/PAN Europe*** (C-615/13P)
  - "The concepts of ***personal data*** and ***data relating to private life*** are not to be confused."
  - a general requirement of transparency stemming from Article 1 TEU, 11(2) TEU and 15 TFEU": not enough
  - "the existence of a climate of suspicion of EFSA, often accused of partiality because of its use of experts with vested interests": yes, disclosure necessary "so that the impartiality of each of those experts could be specifically ascertained"

Further impact of ***Bavarian Lager***

- Regulation 45/2001 becomes applicable **in its entirety**
  - i.e. not only Articles 8 and 9 on "transfers"
  - legal basis for processing of personal data in access to documents cases
  - information to data subjects
  - right to object
- Proactive approach encouraged
  - e.g. 2011 EDPS position paper

The balancing act: other relevant factors

- ***Google Spain*** (C-131/12)
  - publication on the internet, search engines add a new dimension: interconnection, profiling…
  - economic interests (of s. e.) cannot justify the potential seriousness of the interference with data subjects' rights
  - data subjects' rights generally override those of internet users, but the balance may shift depending on the nature of information, role of the individual in public life etc.

EDPS practice (1)

- Verification of postal address of applicants for public access to documents
- Publication of names of EU & EDPS officials in documents released to the public
  - Names/initials and contact details at Head of Unit/Sector level and above are normally disclosed
  - Names, initials, signatures and contact details of staff below HoU/S are redacted in the initial response (necessity can be established in the confirmatory request)
- Publication of personal data in the context of EU Ombudsman inquiries

Outlook

- Regulation 1049/2001: revision process on-going (but blocked)
- Regulation 45/2001: currently under revision (alignment with the GDPR)
  - Article 8 maintained
  - EP LIBE Committee likely to propose changes

Thank you for your attention!

For more information:

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS

Dr Anamarija Musa
Information Commissioner, Croatia
E-mail: povjerenica@pristupinfo.hr

Access to Information and Data Protection in Croatia – An Example of Two Separate Supervisory Bodies

Paper presented at the International Symposium: Data Protection and Freedom of Information – Contradiction or Complement,
Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, Potsdam, 28 September 2017

Abstract: *Transparency and privacy protection are equally important principles of contemporary governance. This paper presents an overview of the institutional models for the protection of access to information and discusses the challenges of combining the protection of access to information and of personal data protection in one institution. The Croatian access to information system is presented as an example that relied on three different models in three distinctive phases of access to information regulation. The combined protection of the right of access to information and of personal data protection in one institution requires a careful institutional design which would prevent the prioritisation of one right over the other and ensure that both are equally protected and promoted among citizens.*

Keywords: access to information, data protection, institutional models, institutional design, Croatia

1. Introduction

Transparency and privacy protection are equally important principles of contemporary governance. The right of access to information[1] and personal data protection as a legal implementation of these principles give citizens the chance to live in countries where they can control the

[1] The term "(right of) access to information" is used as it is more suitable to the contemporary position of access to information. Although in the second half of the 20th century freedom of information was widely used as a legal counterpart to the principle of transparency (freedom of expression and information, Article 10 of the European Convention of Human Rights; freedom of information in USA 1966, etc.) current trends in the European Union and Europe indicate that the "right" of access to information is a more appropriate term. Besides, "one's right" implies that there is an obligation on the other side (here, on the behalf of public authorities).

government and keep their private business safe from the intrusion of others' unwanted attention, especially private companies. In the European Union and in its member states, the two rights have a different position in different legal regimes and administrative traditions. Moreover, the institutional protection of the two rights varies from country to country.

This paper presents the overview of the institutional models for the protection of access to information and discusses the challenges of combining the protection of access to information and personal data protection in one institution. The Croatian access to information system is presented, as an example that relied on three different models in three distinctive phases of the access to information regulation. Finally, the differences and similarities between the two rights are discussed, with an emphasis placed on the challenges of institutional design.

2. On access to Information

Transparency, as the principle of the availability of information about organisations, processes and the decision-making of public authorities, is becoming increasingly important in contemporary governance. It enables the functioning of democratic processes, the functioning of the accountability mechanism, the exercise of individual rights, as well as the overall effectiveness of the public sector. As a consequence, a satisfactory level of transparency and openness is beneficial for the functioning of democracy and public administration, as well as for the individual and for community development.

In the last decades the national legal systems, as well as the European Union,[2] have been adopting laws granting access to public information. Currently, approximately 130 countries, federal units and territories have laws on access to information. The content of the laws and the best examples of specific provisions have been widely discussed and determined in various model laws (e.g. Article 19). The quality of access to information laws is measured, benchmarked and assessed (e.g.

[2] In the European Union, several key legal acts grant the right of access to information: the Charter of Fundamental Rights of the EU, Article 42 Right of access to documents (in force 2009), the Aarhus Convention on Access to Information, Public Participation in Decision Making and Access to Justice in Environmental Matters (United Nations Economic Commission for Europe – UNECE, 1998 (in force 2001), EC Directive on Public Access to Environmental Information 2003/4EC; EU Directive on the Re-use of Public Sector Information 2003/98/EC, 2013/37/EU. The Council of Europe adopted two important documents related to the access to information: the Convention on the access to official documents (signed 2009, not in force), European Charter on Local Self-Government – Protocol on the right to participate in local affairs (signed 2009, in force 2012),

Global RTI ratings), but, as the results show, the quality of legislation in terms of adherence to international standards of procedural safeguards and material quality is not directly linked to the general level of transparency or the absence of corruption.

Importantly, the effectiveness of the laws granting access to information is related to the envisaged enforcement regime. Among others, international standards, as the most important requirement for the enforcement regime, accentuate the existence of an independent institution that is capable to perform its tasks. This independence includes political independence (ensured by the appointment process and the professional ethos), financial and organisational autonomy, and the independence of decision-making. It can be assumed that properly designed independent institutions that have sufficient capacity in terms of funding, personnel and decision-making powers can act as guardians of the integrity of public administration and other public authorities. This applies to other watchdogs of the public interest, such as courts, audit institutions, ombudspersons, ethics committees, etc.

3. Institutional models for the protection of the right of access to information

European countries adopted various institutional models for the protection of the right of access to information. The approach to the institutional choice is dependent on the dominant view on the role of the right of access to information in the legal system and public administration, as well as on the broader setting. This is the consequence of the multi-functionality of the right of access to information which can be approached from different angles: as the citizens' right, as the information right, and as an instrument of good governance, integrity and fighting corruption (Figure 1). Hence, depending on the approach taken, the protection (and the promotion) of the right of access to information can be entrusted to tree different institutional models which are presented in Table 1.

Figure 1: The multi-functionality of the right of access to information

First, the right of access to information can be viewed primarily as *citizens' right*, meaning that it should be protected the same way as other citizens' rights (human rights) – by *the courts* and by the independent protection mechanism such as *ombudsman*. A court procedure follows after the refusal of the request and (usually) an internal review (within the public authority that refused to grant access to information). The ombudsman only has the power of recommendation, thus the ombudsman's decisions are not binding (but are most often followed by the authorities). This model is accepted in Scandinavian countries which were early adopters of access to information laws in 1970s and 1980s, following the example of the United States (1966) and Swedish Freedom of the Press Act of 1766. Another group consists of the Central and Eastern European Countries which adopted the laws in the late 1990s and early 2000s (e.g. Poland, Bulgaria and Romania).

Second, the right of access to information can be understood as an integrative part of *the information rights* such as the data protection right, copyright, the commercial secrecy right, and others. This view supports the idea that the right of access to information could be protected most effectively by an authority that is responsible for other information rights, mostly *personal data protection authorities.* Thus in many European countries it is protected by a special independent authority which is at the same time responsible for personal data protection, be it an agency, a commissioner or a commission, as a collegiate body (e.g. a commissioner in the UK, Slovenia, Switzerland, and Serbia). In some

countries access to information protection can be entrusted to a governmental body, combined with data protection (e.g. German Federal Authority for Data Protection and Freedom of Information until 2014; Estonian, Latvian and Lithuanian Data Inspectorate).

Finally, the access to information can be primarily seen as an instrument that is used to enhance good governance and the integrity of public sectors and which is an important tool for fighting corruption. In this case, it is believed that it is best protected by a specialised independent institution that is exclusively responsible for access to information and related issues, such as open data or public participation. Thus, in some countries commissioners or commissions for access to information are responsible for ensuring the protection and promotion of this right (e.g. commissioners in Ireland,[3] Croatia, Scotland, or a commission in France, Belgium, Italy, Portugal, and Macedonia).

Each type of institution – an ombudsman, a commission(er), an agency or a state administrative body – exerts different institutional features which can lead to different degrees of independence, follows different procedures, and issues different types of decisions. The effectiveness of the institution depends on the broader institutional setting, on political, legal and administrative tradition, on the current political configuration, on the capacity of the institution, etc.

However, the distribution of the types of institutions shows a pattern which could be attributed to the impact of political and administrative tradition: Scandinavian countries prefer an ombudsman type protection combined with court protection, relying strongly on the culture of transparency and the rule of law[4]; the French political and administrative culture breeds mostly commissions exclusively responsible for access to information, but with commissioners appointed by the function (judges, senior civil servants, etc.); while Baltic states prefer state administration to exercise the access to information oversight. The combination of access to information and data protection is well spread in continental law systems, but also in the UK.

[3] A good example of the third approach is the Irish Information Commissioner who is at the same time the Ombudsman and ex an officio member (as an ombudsman) of three important oversight bodies: the Commission for Public Service Appointments, the Referendum Commission and the Standards in Public Office Commission as the head of the Ethics Commission.

[4] Thus, a relative ineffectiveness of the access to information regime in some Eastern European countries might be attributed to the implementation of an institutional model that is not suitable for young democracies still building their political and legal systems.

Table1: The institutional models for the protection of the access to information

Specialisation of functions **Oversight mechanism**	**No specialisation**	**Personal Data Protection & Access to Information**	**Access to Information**
No external administrative appeal mechanism / Ombudsman / Courts control	Sweden, Finland, Norway, Denmark, The Netherlands, Poland, Bulgaria, Romania, Czech Republic, Slovakia, Moldova, Bosnia and Herzegovina		
Governmental body		*Data inspectorate:* Estonia, Latvia, Lithuania	
Independent institution		*Commissioner:* United Kingdom, Germany, Switzerland, Slovenia, Hungary, Albania, Serbia, Malta *Agency* (Commission) Montenegro	*Commissioner:* Ireland, Croatia, Scotland *Commission:* France, Belgium, Portugal Italy, Macedonia Council or Committee: Spain, Iceland

4. The Croatian experience

4.1. Development of the access to information

In Croatia, the access to information regime has developed through three distinctive phases. The first phase (2003-2010) began with the adoption of the first Law on the Right of Access to Information in 2003 as an important step forward in the process of democratization and the reform of the public administration according to European standards. In addition, under the circumstances of an unreformed administrative procedure and justice system and suffering from significant shortcomings with regard to procedural and material elements and the absence of adequate institutional support for the enforcement, the RTI Law has not led to a significant improvement in the overall level of transparency.

The adolescent or intermediate phase (2011-2013) began with the 2011 amendments of the Law, following the introduction of the right of access to information in the Croatian constitution in 2010. The new legislation had significantly improved the access to information regime by broadening the scope of public bodies, as well as the definition of information, by ensuring the better procedural position of the users, and the introduction of the Public Interest Test. But most importantly, as in some other countries, the appeals procedure was designated to an independent institution already responsible for data protection: the Agency for Personal Data Protection. The access to information system of protection was significantly improved and supported by several of the Agency's key decisions, and thus opened the door to the greater transparency of public administration. However, the Agency was still mainly perceived as a data protection institution that was not known for their access to information function to a wider public.

Finally, the mature phase began in 2013 when the new Law was adopted (and amended in 2015), introducing the recent access to information legislation standards regarding the scope of public bodies covered by the Law, the list of exclusions and the Public Interest Test, more effective procedural safeguards, as well as new transparency and openness instruments such as public consultation, and the re-use of public sector information. Moreover, a new, specialised independent body for the protection, monitoring and promotion of the access to information and the re-use of public sector information (open data) was established, with broad formal powers, such as the appellate procedure, investigation and sanctioning. The purpose of this institutional change was to back up the new legislation with a strong institution that would be able to effectively protect and promote access to information, to improve good governance, and to help lower the level of corruption. Civil society played a great role

in promoting the establishment of the specialised independent institution, as did the pressure from the European Union to improve the institutional capacities for fighting corruption and preventing the conflict of interest, as well for the greater transparency.

Table 2: Development of legal framework for the access to information in Croatia

	2003 RTI LAW	*2011 RTI LAW*	*2013/2015 RTI LAW*
Beneficiaries	Any natural or legal person	Any natural or legal person	Any natural or legal person
Bodies bound by law / way of determining the scope	Narrow definition List of public authorities published annually by the Government	Broader definition (incl. public companies, legal persons financed from the public budgets) on a case by case basis	Detailed legal definition Register of Information officers / List of public authorities on a case by case basis
Public interest test	No	Yes classified information – only public authority and the court	Yes At all levels
Appeal	The head of public authority	Agency for Personal Data Protection	Information Commissioner
Judicial control	Administrative court Claimant: beneficiary	Administrative court Claimant: beneficiary Includes silence of administration	High Administrative Court Claimant: beneficiary and public authority Includes silence of administration

	2003 RTI LAW	*2011 RTI LAW*	*2013/2015 RTI LAW*
Inspection control	Part of general administrative inspection (Ministry of Administration)	Part of general administrative inspection (Ministry of Administration)	Information Commissioner
Monitoring and reporting	Report to the Croatian Parliament by Ministry of Administration	Report to the Croatian Parliament by Agency for Personal Data Protection	Report to the Croatian Parliament by the Information Commissioner; other types of monitoring
Proactive disclosure	Yes Catalogue of Information	Yes Proactive publication on the website	Yes Proactive publication on the website
Public consultation	No	No	Yes
Publicity of sessions	Yes	Yes	Yes
Re-use of public sector information	No	No	Yes
Sanctions	Yes	Yes	Yes

Source: adapted from Musa (2018)

4.2. The current practice of the Information Commissioner

The Information Commissioner oversees approximately 6000 public authorities and their compliance with the provisions of the Law on the Right of Access to Information. The Office of the Commissioner (which was established in October 2013) has 12 civil servants (and the Commissioner, the state official), with a budget of 380.000 € per year (2017).[5]

The Information Commissioner is responsible for protecting, monitoring and promoting access to information and the re-use of public sector information (open data), and for monitoring and promoting public consultations and the publicity of sessions of collegiate bodies (e.g. local councils, agency boards, etc.). The instruments it has at its disposal range from the appellate procedure, inspections (in situ or indirectly), procedure upon petitions, monitoring (analytical studies), and promotion instruments (publications, standardisation, education and trainings, events). The overview of the areas and instruments is presented in table 3.

Table 3: Areas and instruments of the Information Commissioner in Croatia

Area (right)	Appeals	Inspections	Petitions	Monitoring & reporting	Promotion
Access to information (request + proactive publication)	✓	✓	✓	✓	✓
Re-use of public sector information (request + proactive publication)	✓	✓	✓	✓	✓
Participation – public consultation		✓	✓	✓	✓
Participation – publicity of sessions		✓	✓	✓	✓

According to the annual reports that public authorities submit to the Information Commissioner in January each year, they receive approximately 20.000 requests for information annually, with a rate of

[5] In 2014, the Office had 4 civil servants, in 2015 it had 7 with three trainees, and in 2016 it had 11 civil servants. Approximately 72% of the budget is spent on salaries and other expenses related to the employees. The size of the budget has been slowly increasing – from 250.000 € in 2014, to over 330.000 € in 2015, 380.000 € in 2016 and 380.000 € in 2017.

92% of all requests being accepted and information disclosed, fully or partially. The Information Commissioner receives between 600 and 650 appeals annually, with 60-65% of appeals being related to silence of administration (not responding in due time, which is 15 calendar days, with an extension up to 30 days). The number of petitions has increased from 59 in 2014 to 324 in 2016 (indicating breaches of the Law by the authorities, for example, by not disclosing certain information on the website). In 2015 and 2016 the Information Commissioner conducted 48 direct inspections (in situ) altogether. The Office manages to close approximately 60% of appeal cases per year.

Table 4: Statistical data

	Office		Appeals					Oversight		
Year	**Civil servants**	**Budget €**	**Appeals (silence of admin)**	**Cases opened**	**Silence of administration**	**Cases closed**	**Rate**	**Petitions**	**Inspections**	**Sanctions**
	No.	.000 €	No.	No.	%	No.	%	No.	No.	No.
2013	4	-	515 (184)	644	64,27	495	76.86	17	0	3
2014	4	200	658 (258)	807	60,79	524	64.93	59	0	4
2015	10	250	624 (222)	609	64,42	528	58.10	211	20	7
2016	11	330	635 (251)	1.015	60,47	674	66.40	324	28	6
2017	12	400	> 1.000	n/a	n/a	584	n/a		n/a	n/a
Total	-	-	**approx. 3.100**			**2.805**		**611**	**48**	**20**

Source: adapted from Musa (2018)

The Information Commissioner and the Agency for Data Protection share some similarities: they are considered to be independent since their heads are appointed by Parliament (the Commissioner is appointed through a public call, the Agency head on the Government's proposal); they submit an annual report to Parliament, and they manage a network of servants responsible for the implementation of the legislation in public authorities (information officers in the area of access to information, data protection officers). For the sake of comparison, in 2016 the Agency for Personal Data Protection had 27 employees (the head and 26 public servants) and the budget of 720.000 €. It dealt with 142 data protection requests, prepared 604 opinions and proceeded upon 417 petitions. It conducted 942 supervisory activities.

5. Highlighting the differences between personal data protection and access to information

Compared to access to information, personal data protection has a slightly different position in European countries and in the European Union (Table 5). Traditionally, the protection of privacy has been a part of the catalogue of constitutionally granted rights (privacy of letters, protection of personal life). Compared to the lack of Europe-wide or EU document or legislation on access to information,[6] as early as in 1981 the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Also, the EU regulated the issue as far back as in 1995 through the Directive, with a new Regulation (GDPR 2016/679/EU) adopted in 2016. Under the Data Protection Directive, during the past 20 years EU countries have created a network of data protection authorities (Article 29 working partially), while access to information conferences and meetings have a more informal character (and are individually funded by participating commissioners).

However, there are many differences between these rights. For example, with regard to the scope of application of the legislation, data protection applies to both the public and the private sector, while access to information solely concerns the public sector (including private sector organisations performing public functions, in some countries). Personal data protection concerns all individuals directly and indirectly, while access to information primarily indirectly affects society and individuals by shedding light on the work and spending of the public sector. In addition, the special interest in the personal data protection regime can

[6] The Council of Europe Convention never came into force and the EU has never adopted a directive or regulation on access to information that would be applicable in the Member states.

be exerted by the IT sector and consultants developing IT and data management systems, while a special interest in access to information is mostly shown by the media and civil sector organisations. The government response in the case of personal data protection ranges from indifferent to active, while when it comes to access to information, governments tend to take a defensive position.

Table 5: Personal data protection and access to information compared

	PERSONAL DATA PROTECTION	ACCESS TO INFORMATION
Beneficiaries	Individual citizens mostly; consumer protection associations and other NGOs	Individual citizens; the media; NGOs, private sector organisations, academia, political parties
Who is concerned?	Anyone (affecting individuals)	Interested public, engaged citizens (but affecting all citizens indirectly)
Who has a special interest?	IT sector, consultants	Media and NGOs
Sphere it concerns	Life in general /public sphere, business	Political life / public sphere
Scope of application	Private sector, public sector; includes media, civil sector organisations	Public sector (including private sector organisations when performing public tasks)
Type of Information	Private and Protected	Public and Disclosed
Government's response (defensive, indifferent, active)	Indifferent to Active	Defensive to Indifferent, sometimes Active
Primary role of the media	Offender	User

	PERSONAL DATA PROTECTION	ACCESS TO INFORMATION
Council of Europe	1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	2009 Convention on the Access to Official Documents (not in force)
EU legislation	Data Protection Directive 1995 Directive on Privacy and Electronic Communications 2002 Charter of Fundamental Rights 2009 (Art 8) GDPR 2016	None obligatory for the MS Charter of Fundamental Rights 2009 (Art 42); Directive on the Re-Use of PSI (2003, 2013); EU Regulation (2001) for EU Institutions
EU institutions and bodies	Data Protection Supervisor	European Ombudsman, among other tasks
MS institutions & Networking	Article 29, http://ec.europa.eu/justice/data-protection/bodies/index_en.htm	None; Conferences of commissioners (informal)

6. Conclusions

There are many reasons that justify the choice of the institutional model that combines the protection of access to information and personal data protection. Both rights fall into the category of the information rights that are crucial in the digital age: on one hand, as individuals we have the right to have our personal data protected from unjustified intrusion, which is easier than ever in contemporary information society; on the other hand, as citizens we have the right of access to public information on the way our public bodies work, on how they make decisions and on what they spend; in the information society, information is and can be accessible easier than ever. The legal frameworks require that supervising authorities for both rights perform their functions in a similar way: they must conduct administrative procedures with binding decisions, issue opinions and recommendations, perform inspections (investigations) and promote these rights in various ways. Moreover, combining the two supervisory functions in one authority saves money in terms of shared supporting services, such as general services, procurement, human resources management, documentation and information management, public relations, etc.

However, there are challenges in performing both tasks in the same institutions. The first challenge relates to the necessity to reconcile conflicting goals and purposes. Privacy protection tends to act secretively, is oriented towards individuals and aims at protecting information from disclosure; in contrast, access to information tends to act as openly as possible, is oriented towards society at large and aims at removing exclusions and exemptions from information.

Thus, as a second challenge, the institutional spirit and organisational cultures might be conflicting among themselves. It is especially critical in cases when the institution has a tradition of protecting one of these rights, and then later acquiring protection of the other right. A cure for that could be an organisational structure that is not formed around the two rights (e.g. the department for data protection and special department for access to information) but rather that is formed according to the type of work (e.g. legal service, investigations, promotion, general services). It could be harder for individual employees to cover different specialities, but it could also be more beneficial for the institutions since it could avoid internal clashes of culture. On the other hand, specialised departments have more power to build an image of the institution as a two-headed monster (for those who breach the law).

Culture clashes and also the prioritisation of one right over the other was or still is more prominent in institutions that do not build the two ‘wings’

equally; it is not uncommon for institutions which have been responsible for data protection for a longer period not to staff their new 'wing' (access to information) soon enough or entirely insufficiently. In this way, the image of the institution still remains in the area of the first right, mostly to avoid change. Institutional adaptation is not easy, and institutional shock may sometimes get absorbed by simply doing nothing. An imbalance between the two rights that is not solved at the beginning only perpetuates the problems of the unequal position of the two rights which was explained in the previous chapter. It is especially challenging in EU member states, where data protection has obtained a much better position when it comes to a legal framework and institutional set-up at the EU level.

Furthermore, it could be expected that in the future, privacy and data protection will be given priority, given the challenges of the digital age, the accelerated and complex development of data protection regimes in relation to technology (the pressures from the IT sector), and ordinary citizens' personal interest in privacy. On the other hand, given the fact that the golden age of the promotion of good governance is in decline, it is not unexpected that we will witness the closing-up of governments; global business interests and global security concerns, as well as political changes towards populist and extreme politics, point in this direction. In any case, the organisational design of the combined institution is the most crucial issue if we want citizens' right to be equally treated, protected and promoted by a strong institution in the digital age.

Bibliography

MUSA, A. (2018, *forthcoming*) Croatia: Transparency Landscape. In: Dragos, D., Kovač, P., Marseille, B., eds. The Laws of Transparency In Practice. Palgrave MacMillan

MUSA, A. (2016) Integrity and free access to information. Croatian experience. In: Meyer-Sahling, J.H., ed. The Professionalisation of Civil Service between Politics and Administration, 8th RESPA Annual Conference proceedings, 12-13 November 2015, Danilovgrad, Montenegro. Danilovgrad, Montenegro: Regional School of Public Administration, pp. 95-110

MUSA, A., JURIĆ, M. & MATAIJA, M. (2011) Transparency and Data Protection in the Context of E-government. Two case studies. In: van Dijk & Jožanc, N. eds., Information Society and Globalization: Transformation of Politics. Conference Proceedings. Zagreb: CIP, pp. 175-207.

ASSET DECLARATION OF CIVIL SERVANTS AND POLITICIANS –

PERSONAL DATA AND THE PREVENTION OF CORRUPTION

Oleksandr Kalitenko
Policy analysis expert
Transparency International Ukraine

International Symposium "Data Protection and Freedom of Information – Contradiction or Complement?“, 28 September 2017, Potsdam

THE STATUS OF CORRUPTION IN UKRAINE

Corruption in Ukraine is an actual threat to state security. It is defined in:

- Article 7 of the Law of Ukraine "On the Fundamentals of National Security of Ukraine“,
- Paragraph 3.3 of Part 3 of the Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 "On the Strategy of National Security of Ukraine”

Said Strategy emphasizes the need to ensure the purge of power from corrupt officials and agents of foreign special services, nonprofessionals, political influence, and the impossibility of predominance of personal, corporate, and regional interests over national ones.

Violation of the right to non-interference in the private and family life of the declarant?

- Constitution of Ukraine; Aarhus Convention 1998; Recommendations of the Parliamentary Assembly of the Council of Europe (PACE) No. 854
- Article 19 of the Universal Declaration of Human Rights, article 19 of the International Covenant on Civil and Political Rights; Article 10 of the European Convention on Human Rights: "freedom ... to receive ... information“
- Recommendation No. R (81) 19 of the Committee of Ministers of the Council of Europe on access to information
- ECHR: Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung eines wirtschaftlich gesunden land- und forstwirtschaftlichen Grundbesitzes (OVESSG) v. Austria (28.11.2013)
- Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data

Guarantees against excessive interference by the state

- the possibility granted to the subject of the declaration to explain the differences in the declaration and to correct such a discrepancy within 5 or 7 days (Part 2 of Article 58, Part 4 of Article 45 of the Law “On Corruption Prevention”);
- the possibility granted to the subject of the declaration to provide an explanation of the established fact of inconsistency of living standards with income (Part 4 of Article 51 of the Law);
- the right to appeal to the court in case of violation of their rights, in accordance with the procedure established by the Code of Administrative Justice of Ukraine;
- the right of the subject of the declaration and third parties to compensation for damage caused as a result of illegal decisions, actions or inactivity of the NAPC (Article 2, Article 68 of the Law).

Does the content of the right to private and family life apply equally to persons authorized to perform functions in the government or local self-government and those who do not perform such functions?

- Resolution of the Plenum of the Supreme Court of Ukraine dated 27.02.2009
- Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe
- ECHR: Karhuvaara and Iltalehti v. Finland; Porubova v. Russia; Von Hannover v. Germany; Aleksey Ovchinnikov v. Russia; Lingens v. Austria; Axel Springer v. Germany; Leander v. Sweden; Malone v. The United Kingdom; Wypych v. Poland etc.

The inadmissibility of requirement to the declarant to indicate information about the property status of family members?

Family members are often used by unscrupulous officials to hide wealth, and in this regard, the current legislation provides for the obligation to declare their status as well.

The Law of Ukraine "On the Prevention of Corruption" does not provide for the obligation of family members to inform the declarant about their available wealth. At the same time, this Law imposes an obligation to obtain this information directly on the declarant, since he has the necessary legal personality with respect to family members in order to obtain the information necessary for the declaration of income. In the event of a family member refusing to provide the required information about the estate, the declarant may file a declaration without such information.

Possible disclosure of a medical secret?

The declarant may not specify personal data while describing the transaction.

Thus, this information will not be available in the public space, which will enable personalization of a particular medical service.

The NAPC may ask the declarant for such data, but in this situation, the relevant NAPC employee who receives such data will potentially be held liable under Article 145 of the Criminal Code of Ukraine "Illegal disclosure of medical secrets“.

Monitoring of the lifestyle – investigative actions?

- Implementation of the GRECO Recommendation on the results of the Joint First and Second Rounds of Evaluation,
- Implementation of the relevant recommendations of European Commission experts within the implementation of the Action Plan on the Liberalization of the European Union Visa Requirements for Ukraine
- Implementation of Article 6 of the UN Convention against Corruption to ensure the establishment and functioning of an anti-corruption policy body

The law contains clear requirements for its implementation:

- regarding the purpose of such monitoring, namely, the conformity of their living standards with the property and income received by declarants and their family members according to the declaration
- regarding the grounds and object of monitoring, namely, information received from individuals and legal entities, as well as from the mass media and other open sources of information, which contains information about the inconsistency of the living standards to declared assets and income
- regarding the need to determine the procedure for monitoring the lifestyle of subjects of declaration by the NACP
- the clear limits of monitoring lifestyle, compliance with legislation on the protection of personal data and restrictions on excessive interference with the right to privacy of a person; potential criminal liability for abuse of power

Potential robbery and kidnapping?

Although there is no separate statistics on property crimes against public officials, the police did not report any increase in the number of crimes against public officials after declarations and the registry of real estate property became public.

Cases of Latvia, Moldova and Romania, where similar requirements on assets disclosure for public officials have never been reported to cause any security concerns.

Thank you for your attention

kalitenko@ti-ukraine.org
+ 380 95 50 20 610
ti-ukraine.org/en
transparency.org

LEUPHANA
UNIVERSITÄT LÜNEBURG

Datenschutz und Informationsfreiheit – Widerspruch oder Ergänzung?
Data Protection and Freedom of Information – Contradiction or Complement?

Der Umgang mit personenbezogenen Daten im Umweltinformationsrecht
The Treatment of Personal Data within the Environmental Information Law

Thomas Schomerus

Potsdam, 28. September 2017

LAND BRANDENBURG
LDA
Schutz der
• Persönlichkeitsrechte
• Informationsfreiheit

Inhalt

- **Einführung:**
  - Datenschutz und Informationsfreiheit – natürliche Gegner?
- **Hauptteil:**
  - Informationsfreiheit und Datenschutz am Beispiel des UIG
- **Schluss:**
  - Datenschutz und Informationsfreiheit – natürliche Verbündete!

Einführung:
Datenschutz und Informationsfreiheit – natürliche Gegner?

- **Informationsfreiheitsrecht**
  - Verfolgung öffentlicher Zwecke wie
    - Demokratie (IFG),
    - Umweltschutz (UIG) oder
    - Verbraucherschutz (VIG)

    durch Herausgabe von Daten (**Transparenz)**

§ 1 Abs. 1 UIG:
Zweck dieses Gesetzes ist es, den rechtlichen Rahmen für den **freien Zugang zu Umweltinformationen** bei informationspflichtigen Stellen sowie für die Verbreitung dieser Umweltinformationen zu schaffen.

- **Datenschutzrecht**
  - Verfolgung des individualbezogenen Zwecks
    - Schutz des Persönlichkeitsrechts

    durch Nicht-Herausgabe von Daten (**Geheimhaltung)**

§ 1 Abs. 1 BDSG:
Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen **personenbezogenen Daten in seinem Persönlichkeitsrecht** beeinträchtigt wird.

Nach den Grundrechtskatalogen des Völker- und Unionsrechts sind Informationsfreiheit und Datenschutz grundsätzlich gleichrangig.

- **Völkerrecht (Allgemeine Erklärung der Menschenrechte)**
  - keine explizite Nennung von Informationsfreiheit und Datenschutz, aber Art. 1 (Würde) und 3 (Freiheit) sowie 19 (Meinungsfreiheit)

- **Unionsrecht (EU-Grundrechtecharta)**
  - freier Zugang zu (Umwelt-)Informationen bei Behörden und Schutz personenbezogener Daten basieren auf Grundrechten und stehen grds. auf einer Stufe

Artikel 42 EU-Grundrechtecharta
Recht auf Zugang zu Dokumenten
Die Unionsbürgerinnen und Unionsbürger sowie jede natürliche oder juristische Person mit Wohnsitz oder satzungsmäßigem Sitz in einem Mitgliedstaat haben das **Recht auf Zugang zu den Dokumenten** der Organe, Einrichtungen und sonstigen Stellen der Union, unabhängig von der Form der für diese Dokumente verwendeten Träger. **(s. auch Art. 15 Abs. 3 AEUV)**

Artikel 8 EU-Grundrechtecharta (auch Art. 16 Abs. 1 AEUV)
Schutz personenbezogener Daten
(1) Jede Person hat das Recht auf **Schutz der sie betreffenden personenbezogenen Daten**.

Im Umweltinformationsrecht wird der Datenschutz aber als Ausnahme vom Grundsatz des freien Zugangs zu Informationen gesehen.

- **Völkerrecht (Aarhus-Konvention)**
  - Regel: Recht auf Zugang zu Informationen über die Umwelt (Art. 4 Abs. 1)
  - (optionale) Ausnahme: Datenschutz Art. 4 Abs. 4 f)
- **Unionsrecht (Umweltinformationsrichtlinie – UIRL):**
  - Regel: freier Zugang zu (Umwelt-)Informationen bei Behörden (Art. 3 Abs. 1)
  - (optionale) Ausnahme: Vertraulichkeit personenbezogener Daten (Art. 4 Abs. 2 f)

Artikel 3 UIRL
Zugang zu Umweltinformationen auf Antrag
(1) Die Mitgliedstaaten gewährleisten, dass Behörden gemäß den Bestimmungen dieser Richtlinie verpflichtet sind, die bei ihnen vorhandenen oder für sie bereitgehaltenen **Umweltinformationen allen Antragstellern auf Antrag zugänglich zu machen**, ohne dass diese ein Interesse geltend zu machen brauchen.

Artikel 4 UIRL
(2) Die **Mitgliedstaaten können vorsehen**, dass ein Antrag auf Zugang zu Umweltinformationen abgelehnt wird, wenn die Bekanntgabe **negative Auswirkungen** hätte auf: …
f) die **Vertraulichkeit personenbezogener Daten** und/oder Akten über eine natürliche Person, sofern diese der Bekanntgabe dieser Informationen an die Öffentlichkeit nicht zugestimmt hat und sofern eine derartige Vertraulichkeit nach innerstaatlichem oder gemeinschaftlichem Recht vorgesehen ist;…

4

Hauptteil: Informationsfreiheit und Datenschutz am Beispiel des UIG

Das Umweltinformationsgesetz folgt dem Regel-Ausnahme-Verhältnis von Aarhus-Konvention und UIRL.

- **Auslegungsregeln**:
  - Grundsatz der Informationsfreiheit: weite Auslegung
  - Ausnahme des Datenschutzes: enge Auslegung
- BVerfG, Urteil vom 15. 12. 1983 – 1 BvR 209/83 (**Volkszählungsurteil**):
  - keine schrankenlose Gewährleistung des Rechts auf informationelle Selbstbestimmung
    - Information als Abbild sozialer Realität
    - Spannung Individuum – Gemeinschaft
    - Einzelner muss „Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen“

§ 1 UIG Zweck des Gesetzes; Anwendungsbereich
(1) Zweck dieses Gesetzes ist es, den rechtlichen Rahmen für den **freien Zugang zu Umweltinformationen** bei informationspflichtigen Stellen sowie für die Verbreitung dieser Umweltinformationen zu schaffen.

§ 9 UIG Schutz sonstiger Belange
(1) Soweit
1. durch das Bekanntgeben der Informationen **personenbezogene Daten** offenbart und dadurch Interessen der Betroffenen erheblich beeinträchtigt würden,…

ist der Antrag abzulehnen, es sei denn, die Betroffenen haben **zugestimmt** oder das **öffentliche Interesse an der Bekanntgabe** überwiegt.

Der Begriff der personenbezogenen Daten ist aber nach den Regeln des Datenschutzrechts weit auszulegen.

- **persönliche und sachliche Verhältnisse einer natürlichen Person**
  - umfasst jede Aussage unabhängig von der Sensibilität
  - Problem: Geodaten – Aussage über Grundstückseigentümer?
    - VG Potsdam, Urteil vom 11. 04. 2014 (rechtskräftig):
      - Zuordnung einer Person zu einem Flurstück nur bei Zusatzwissen wie Zugriff auf Grundbuch
      - Folge: keine personenbezogenen Daten
    - Kritik (vgl. Götze, LKV 2013, 241):
      - für Einsicht in das Grundbuch „berechtigtes Interesse“ ausreichend – geringe Hürde
      - s. auch EuGH, Urt. v. 9. 11. 2010 – C-92/09 (Agrarbeihilfen)

§ 3 Abs. 1 BDSG:
(1) Personenbezogene Daten sind **Einzelangaben über persönliche oder sachliche Verhältnisse** einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

EuGH, Urt. vom 9.11.2010, C-92/09:
„Dem Ziel der Transparenz kann insoweit **nicht ohne Weiteres Vorrang** gegenüber dem Recht auf Schutz der personenbezogenen Daten zuerkannt werden, selbst wenn erhebliche wirtschaftliche Interessen betroffen sind.“

Darf die Herausgabe von Informationen nach § 9 Abs. 1 Nr. 1 UIG nur verweigert werden, wenn durch die Veröffentlichung über den durch die Datenschutzgesetze gewährten Schutz zusätzliche erhebliche Beeinträchtigungen hinzukommen?

- **Ja**:
  - OVG Berlin-Brandenburg, Urt. v. 12.02.2015 – OVG 12 B 13/12 (Geodaten):
    - „gesetzliche(s) Regel-Ausnahme-Verhältnis zwischen freiem Informationszugang und Versagungsgründen“
    - „erhebliche(n) Beeinträchtigung der Interessen der Betroffenen“ erforderlich
- **Nein**:
  - VG Karlsruhe, Urteil v. 27.05.2013, 2 K 3249/12 (Löschung von Daten des ehem. Ministerpräsidenten):
    - „Antrag auf Zugang zu Umweltinformationen“ sperrt „die Löschung der E-Mail-Postfachdaten nicht“
    - kein Fall der „Entziehung des Informationsanspruchs“ durch Datenlöschung
- **Ergebnis**:
  - ja, da Wortlaut des § 9 Abs. 1 S. 1 Nr. 1 UIG („und“) nicht nur das Vorliegen personenbezogener Daten, sondern zusätzlich eine erhebliche Beeinträchtigung der Interessen des Betroffenen voraussetzt

Erteilt der Betroffene keine Einwilligung, hat die informationspflichtige Stelle eine eigene Abwägung zwischen dem privaten Interesse des Betroffenen und dem öffentlichen Interesse an der Bekanntgabe vorzunehmen.

- Antragsteller ist **Repräsentant der Öffentlichkeit**, kommt daher nicht auf spezifisches Individualinteresse an!
- überwiegendes öffentliches Interesse z. B. aus **Aufgabennormen** abzuleiten wie immissions- oder atomrechtliche Überwachungsvorschriften
- je gefährlicher z.B. eine **Anlage**, desto höher das öff. Interesse
- VGH Kassel, Beschluss vom 31. Oktober 2013 – 6 A 1734/13.Z – Freisetzung von gent. veränd. Organismen
  - Behörde muss **Schutzgründe** geltend machen und substantiiert nachweisen
  - keine **Schutzwürdigkeit** von Name, Beruf und Dienststellung
  - aber schutzwürdiges Interesse an Geheimhaltung von **persönlichen Daten** wie Gehaltsauszügen, Kontoverbindungen, Reisekosten und Mitteilungen über persönliche Verhältnisse

§ 9 Abs. 1 Satz 1 UIG:
…ist der Antrag abzulehnen, es sei denn, die Betroffenen haben zugestimmt oder das öffentliche Interesse an der Bekanntgabe überwiegt.

Bei dem „Public-Interest-Test“ hat daher in jedem Einzelfall eine Ermittlung, Bewertung und Gewichtung der dem Informationsbegehren gegenüberstehenden Datenschutzbelange zu erfolgen.

- zu beachten, dass Datenschutz über das Recht auf informationelle Selbstbestimmung **Grundrechtscharakter** genießt
- auch legitime **wirtschaftliche Belange** können zu berücksichtigen sein (OLG Köln, Urteil vom 15. 12. 2006 – 6 U 229/05)
- auch zu klären, ob Antragsteller in erster Linie **Umweltschutzinteressen** oder eigene Interessen verfolgt

> BVerwG, Urteil vom 24. 9. 2009 – 7 C 2.09:
> „Die Kl. verfolgt damit aber in erster Linie eigene Interessen. Ein Nutzen für den Umweltschutz ergibt sich allenfalls als Nebenprodukt. Zwar ist das System des Emissionshandels wegen seiner Bedeutung für den Klimaschutz von herausgehobenem öffentlichen Interesse. An diesem herausgehobenen öffentlichen Interesse haben aber Informationen über zwei Beteiligte dieses Handelssystems wegen ihrer geringen Aussagekraft für das Funktionieren des Systems insgesamt nur wenig Bedeutung.“

- kommt auch darauf an, wer **Antragsteller** ist (Fluck, DVBl 2006, 1406, aber zweifelhaft!)
- ggf. teilweise **Anonymisierung** erforderlich (OVG Münster, Urteil vom 20. 6. 2005 – 8 B 940/05) – s. auch § 5 Abs. 3 UIG

Für Umweltinformationen über Emissionen gilt eine weitere Rück-Ausnahme.

- enge oder weite Auslegung des Begriffs der Emissionen?
- VG Darmstadt, Urteil vom 10. 05. 2017, 6 K 695/16.DA:
  - „Unter einer Umweltinformation über Emissionen ist ausschließlich die Information darüber zu verstehen, **welche Stoffe in welcher Menge eine Anlage verlassen** und in diesem Sinne in die Umwelt freigesetzt werden. Hingegen fallen unter den Begriff der Umweltinformation über Emissionen noch nicht Informationen über Vorgänge innerhalb der Anlage, durch die die später in die Umwelt abgegebenen Stoffe entstehen oder deren Zusammensetzung und Menge beeinflusst werden ... Die vereinbarte Abschaltregelung hat zwar Einfluss auf die Dauer des Betriebs der WEA und damit auf die Menge der von ihr ausgehenden Emissionen, stellt jedoch selbst keine Emission dar.“

§ 9 Abs. 1 Satz 2 UIG
Der Zugang zu Umweltinformationen über **Emissionen** kann nicht unter Berufung auf die in den Nummern 1 und 3 genannten Gründe abgelehnt werden.

Für Umweltinformationen über Emissionen gilt eine weitere Rück-Ausnahme.

- enge oder weite Auslegung des Begriffs der Emissionen?
- VG Darmstadt, Urteil vom 10. 05. 2017, 6 K 695/16.DA:
  - „Unter einer Umweltinformation über Emissionen ist ausschließlich die Information darüber zu verstehen, **welche Stoffe in welcher Menge eine Anlage verlassen** und in diesem Sinne in die Umwelt freigesetzt werden. Hingegen fallen unter den Begriff der Umweltinformation über Emissionen noch nicht Informationen über Vorgänge innerhalb der Anlage, durch die die später in die Umwelt abgegebenen Stoffe entstehen oder deren Zusammensetzung und Menge beeinflusst werden ... Die vereinbarte Abschaltregelung hat zwar Einfluss auf die Dauer des Betriebs der WEA und damit auf die Menge der von ihr ausgehenden Emissionen, stellt jedoch selbst keine Emission dar.“

§ 9 Abs. 1 Satz 2 UIG
Der Zugang zu Umweltinformationen über **Emissionen** kann nicht unter Berufung auf die in den Nummern 1 und 3 genannten Gründe abgelehnt werden.

Nach den meisten Umweltinformationsgesetzen haben die Beauftragten für Datenschutz und Informationsfreiheit keine Beratungs-, Kontroll- und Berichtskompetenzen wie im Falle der Datenschutz- und Informationsfreiheitsgesetze.

- Schade!
  - keine Unterstützung von Antragstellern nach UIG zulässig
  - keine Vermittlung oder Kontrolle in Streitfällen
  - keine Anrufung des Beauftragten bei Ablehnung von Anträgen

> Tätigkeitsbericht LDA Brandenburg 2014/2015, S. 179: „Die gesetzliche Kompetenz der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht erstreckt sich **ausschließlich auf die Wahrung der Rechte nach dem Akteneinsichts- und Informationszugangsgesetz**."

- denn: Beauftragte für Datenschutz und Informationsfreiheit wären gerade für Fragen des Datenschutzes als Ausnahmetatbestand prädestiniert

Schluss:

Datenschutz und Informationsfreiheit sind keine natürlichen Gegner, sondern natürliche Verbündete!

- **Vorrangverhältnis?**
  - kein Vorrang des Datenschutzes vor der Informationsfreiheit
  - aber auch kein Vorrang der Informationsfreiheit vor dem Datenschutz
  - der Einzelfall ist entscheidend!

- **Informationsfreiheit bedingt Datenschutz**
  - ohne Datenschutz keine Akzeptanz für Informationsfreiheit
  - Abwägung im Sinne einer praktischen Konkordanz erforderlich

> "The Data Protection Act exists to protect people's right to privacy, whereas the Freedom of Information Act is about getting rid of unnecessary secrecy. These two aims are **not necessarily incompatible** but there can be a tension between them, and applying them sometimes **requires careful judgement**. "
> Information Commissioner´s Office, What is the Freedom of Information Act? (https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/)

Ich freue mich auf Ihre Fragen.

Herzlichen Dank für Ihre Aufmerksamkeit!

Univ.-Prof. Dr.
Thomas Schomerus RiOVG
Leuphana University
Lueneburg, Germany
schomerus@leuphana.de

Quelle: http://www.leuphana.de/news/meldungen-forschung/ansicht/datum/2017/08/28/energieforum-der-wind-schreibt-keine-rechnungen.html

INFORMATION AND
DATA PROTECTION
COMMISSIONER
Proactive Publication of Public Sector
Information on the Internet
The Example of an Albanian Platform

FOIA IN ALBANIA

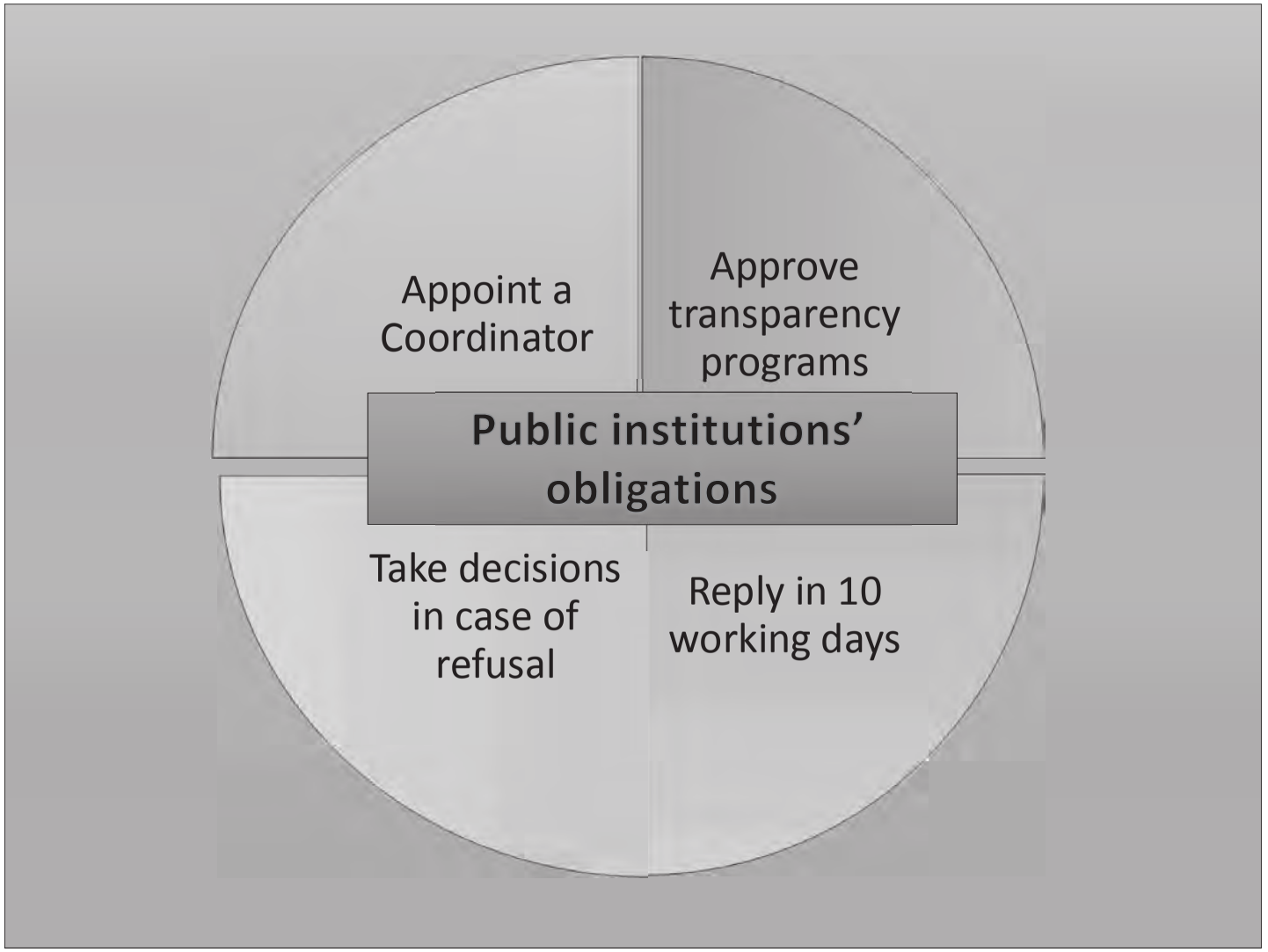
Constitutional right

The first FOIA law: 1998

The actual law: 2014

RTI 6 position

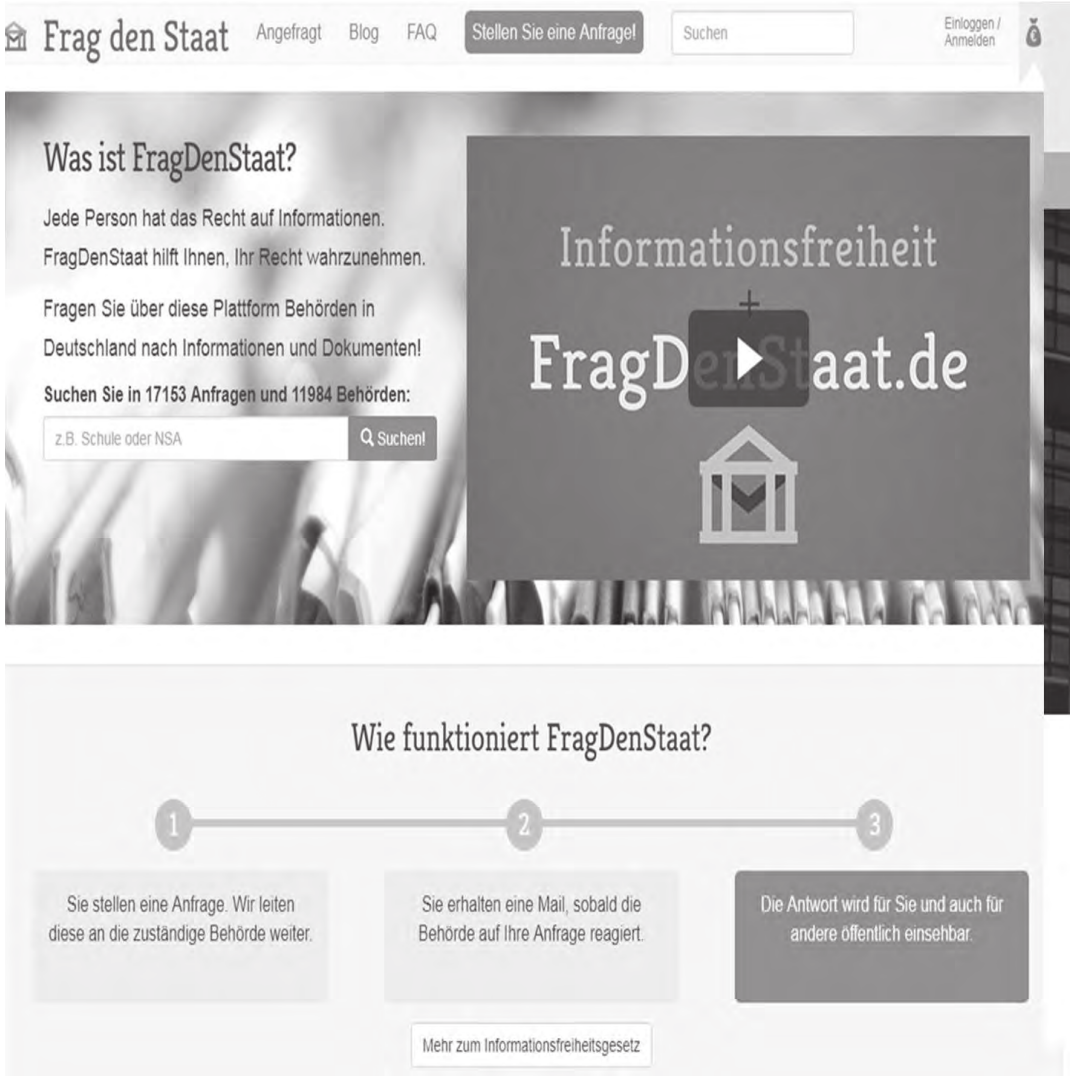
INFORMATION AND DATA PROTECTION COMMISSIONER

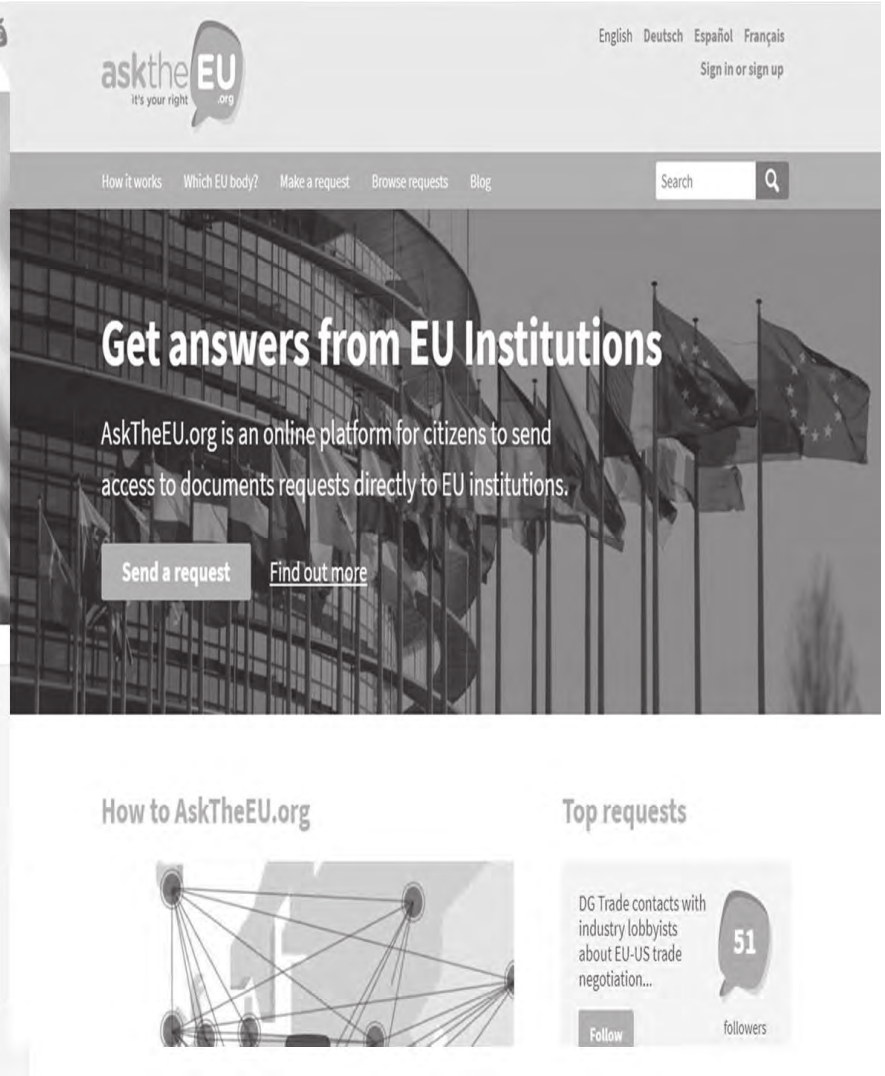

Appoint a Coordinator
Approve transparency programs
Public institutions' obligations
Take decisions in case of refusal
Reply in 10 working days

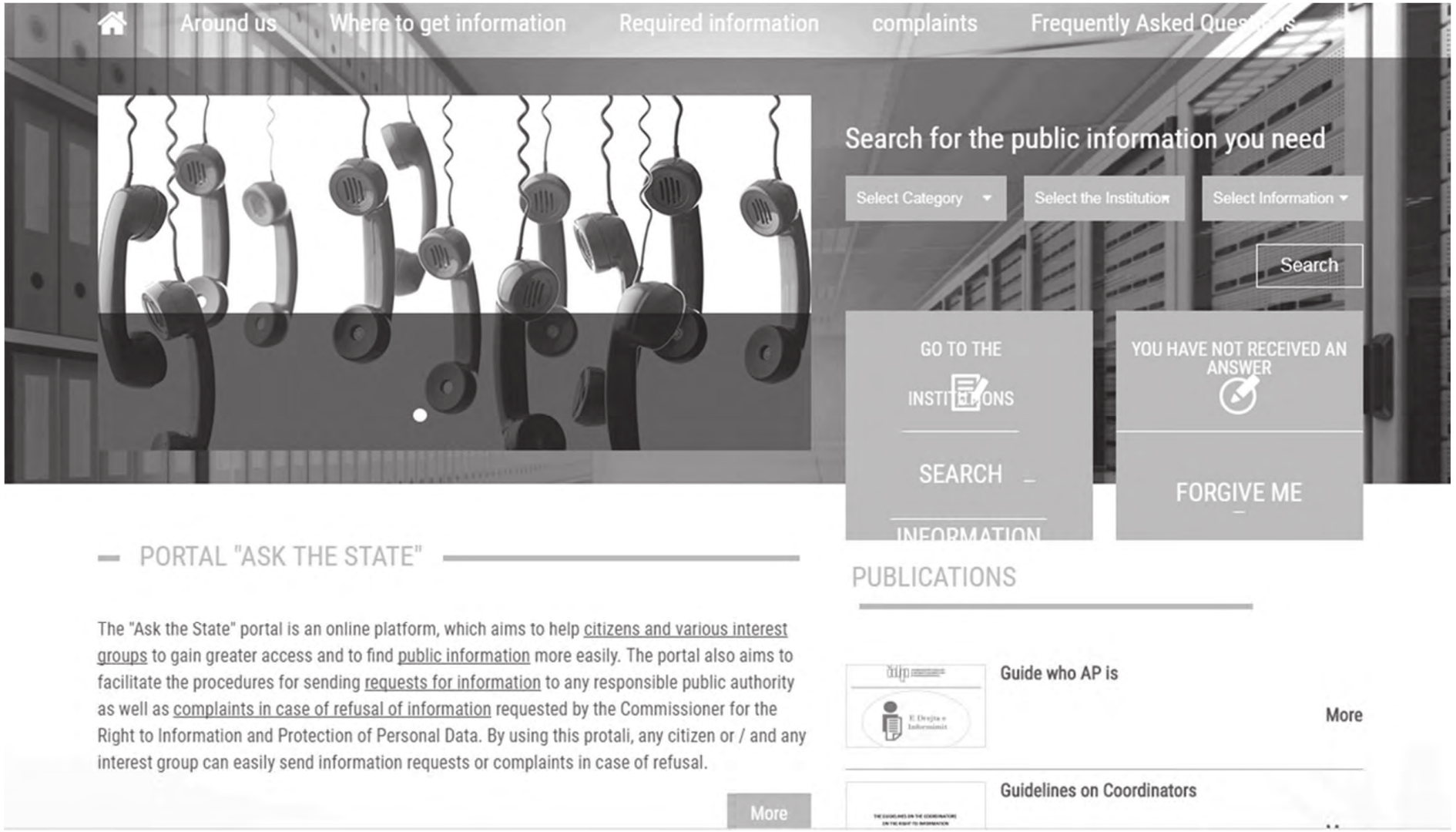
TRANSPARENCY PROGRAM = PROACTIVE DISCLOSURE

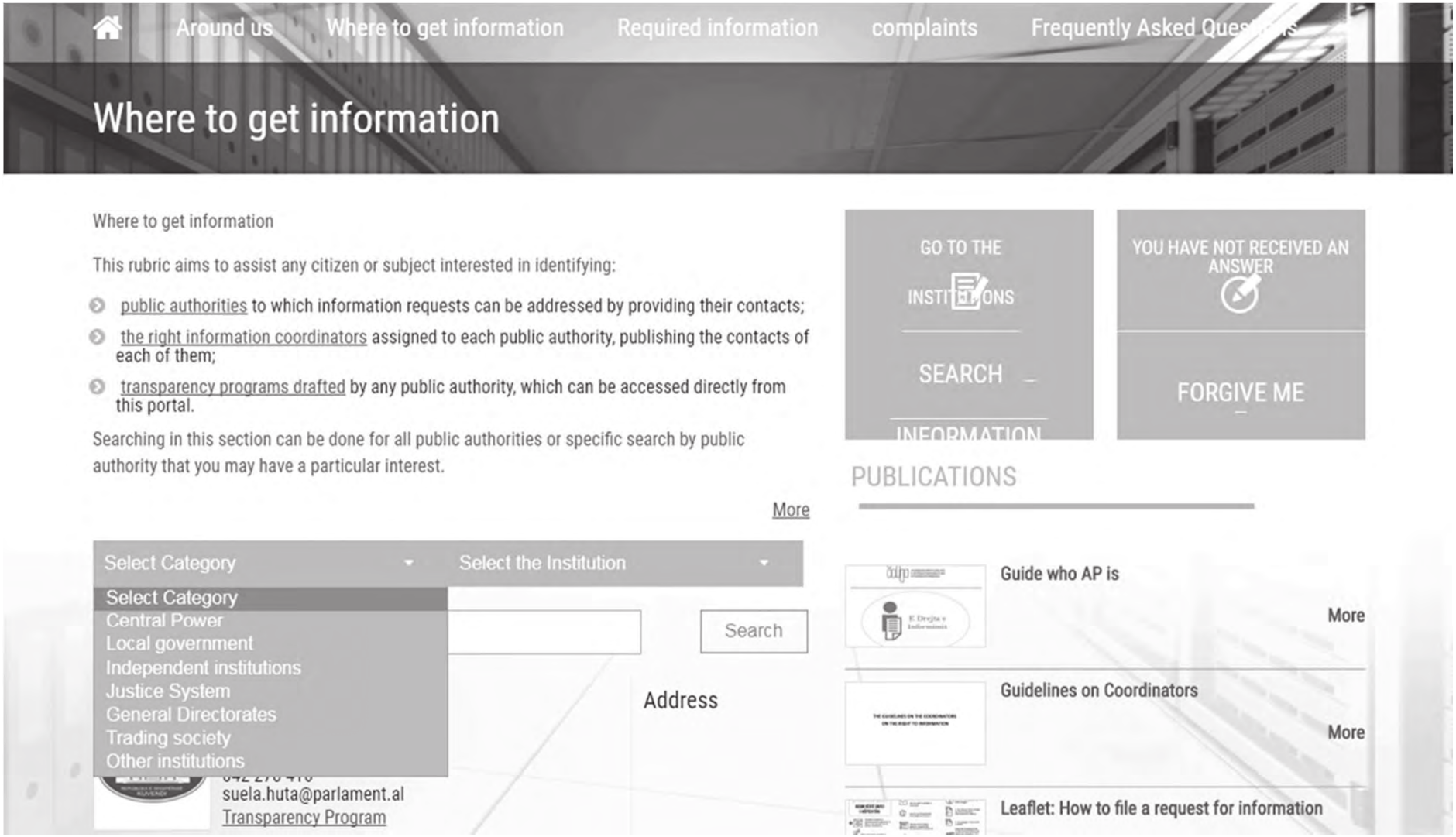
1. Law
2. Budget
3. Public Procurement
4. Contracts
5. Organigram of the institution
6. Audit reports
7. Register of requests = Access to one, access to all

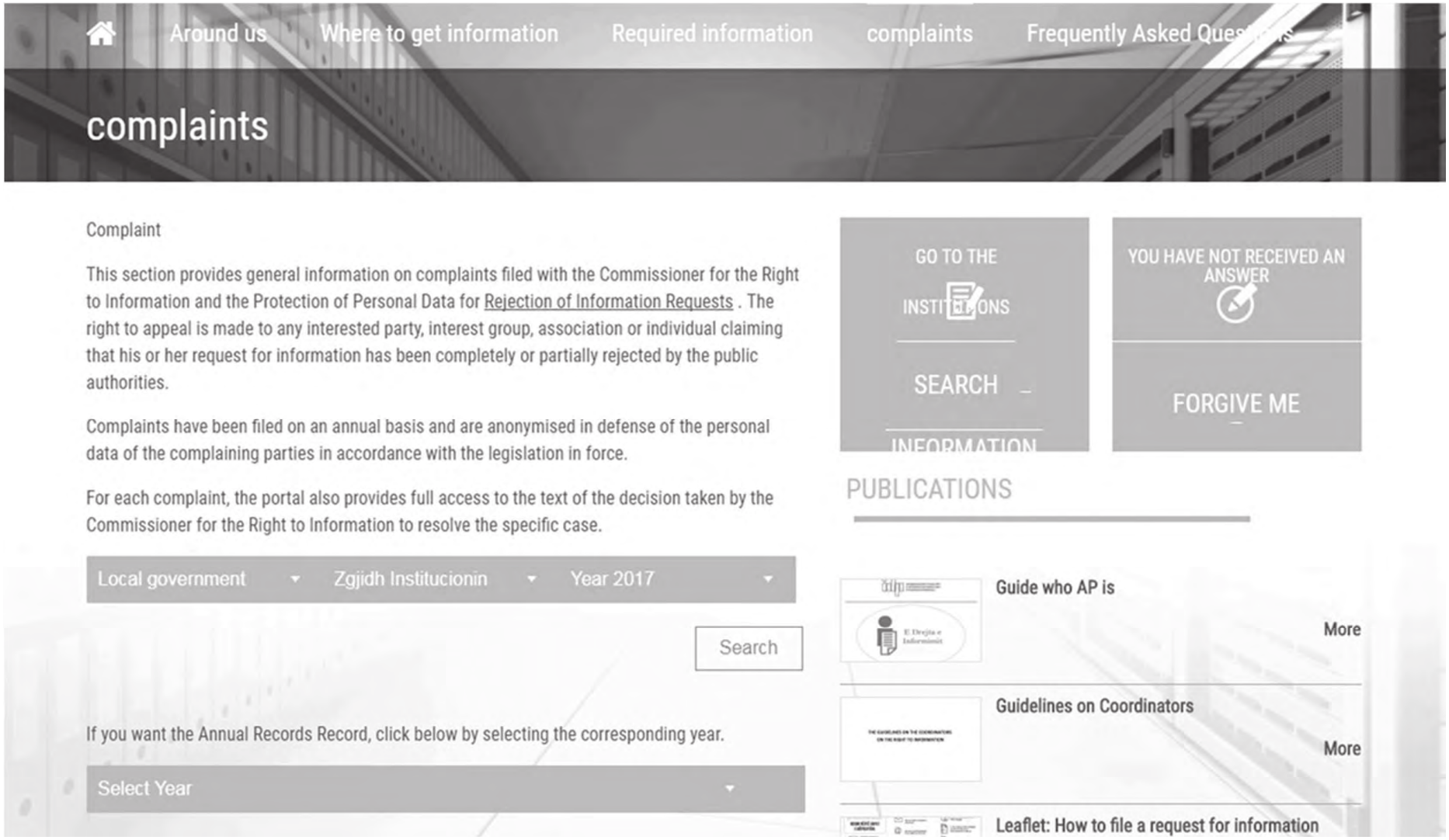
INFORMATION AND DATA PROTECTION COMMISSIONER


Frag den Staat
Angefragt
Blog
FAQ
Stellen Sie eine Anfrage!
Suchen
Einloggen / Anmelden
Was ist FragDenStaat?
Jede Person hat das Recht auf Informationen.
FragDenStaat hilft Ihnen, Ihr Recht wahrzunehmen.
Fragen Sie über diese Plattform Behörden in Deutschland nach Informationen und Dokumenten!
Suchen Sie in 17153 Anfragen und 11984 Behörden:
z.B. Schule oder NSA
Suchen!
Informationsfreiheit
FragDenStaat.de
Wie funktioniert FragDenStaat?
1
2
3
Sie stellen eine Anfrage. Wir leiten diese an die zuständige Behörde weiter.
Sie erhalten eine Mail, sobald die Behörde auf Ihre Anfrage reagiert.
Die Antwort wird für Sie und auch für andere öffentlich einsehbar.
Mehr zum Informationsfreiheitsgesetz

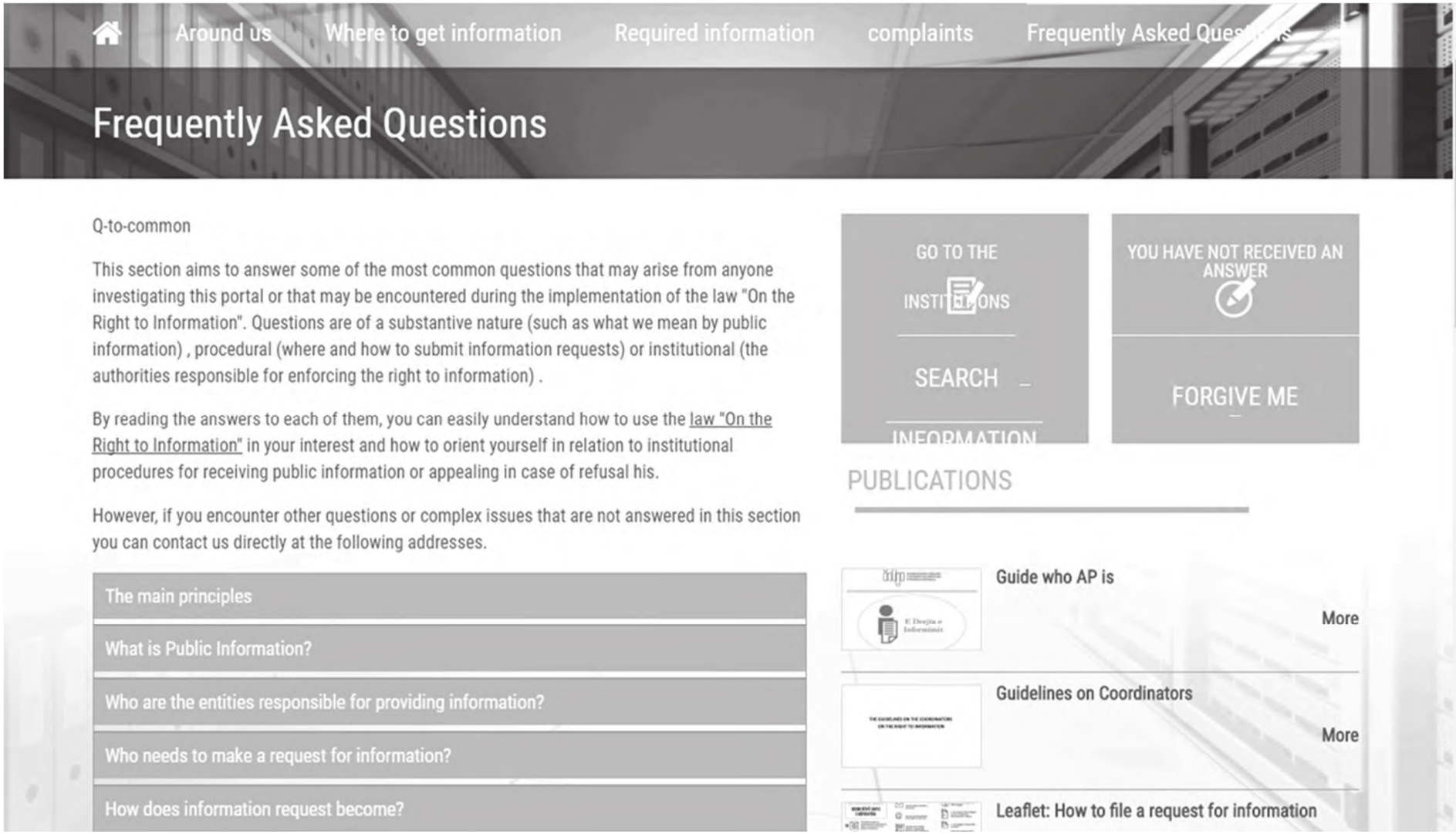

askthe EU
it's your right .org
English
Deutsch
Español
Français
Sign in or sign up
How it works
Which EU body?
Make a request
Browse requests
Blog
Search
Get answers from EU Institutions
AskTheEU.org is an online platform for citizens to send access to documents requests directly to EU institutions.
Send a request
Find out more
How to AskTheEU.org
Top requests
DG Trade contacts with industry lobbyists about EU-US trade negotiation...
51
Follow
followers

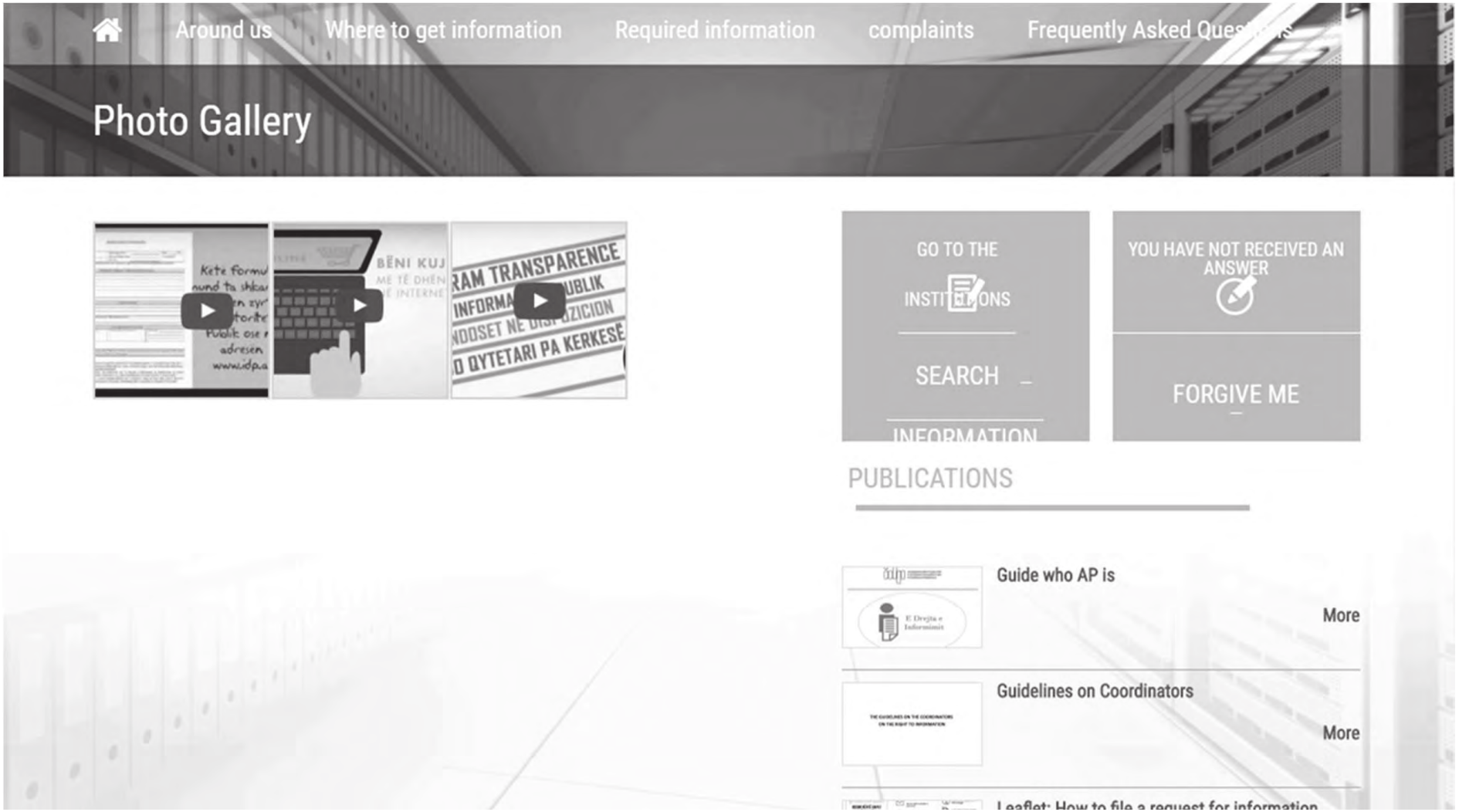

Around us
Where to get information
Required information
complaints
Frequently Asked Ques
Search for the public information you need
Select Category
Select the Institution
Select Information
Search
GO TO THE
INSTITUTIONS
SEARCH
INFORMATION
YOU HAVE NOT RECEIVED AN ANSWER
FORGIVE ME
PORTAL "ASK THE STATE"
The "Ask the State" portal is an online platform, which aims to help citizens and various interest groups to gain greater access and to find public information more easily. The portal also aims to facilitate the procedures for sending requests for information to any responsible public authority as well as complaints in case of refusal of information requested by the Commissioner for the Right to Information and Protection of Personal Data. By using this protali, any citizen or / and any interest group can easily send information requests or complaints in case of refusal.
More
PUBLICATIONS
Guide who AP is
More
Guidelines on Coordinators


Around us
Where to get information
Required information
complaints
Frequently Asked Questions
Where to get information
Where to get information
This rubric aims to assist any citizen or subject interested in identifying:
public authorities to which information requests can be addressed by providing their contacts;
the right information coordinators assigned to each public authority, publishing the contacts of each of them;
transparency programs drafted by any public authority, which can be accessed directly from this portal.
Searching in this section can be done for all public authorities or specific search by public authority that you may have a particular interest.
More
Select Category
Select the Institution
Select Category
Central Power
Local government
Independent institutions
Justice System
General Directorates
Trading society
Other institutions
Search
Address
suela.huta@parlament.al
Transparency Program
GO TO THE INSTITUTIONS
SEARCH INFORMATION
YOU HAVE NOT RECEIVED AN ANSWER
FORGIVE ME
PUBLICATIONS
Guide who AP is
More
Guidelines on Coordinators
More
Leaflet: How to file a request for information


Around us
Where to get information
Required information
complaints
Frequently Asked Questions
complaints
Complaint
This section provides general information on complaints filed with the Commissioner for the Right to Information and the Protection of Personal Data for Rejection of Information Requests . The right to appeal is made to any interested party, interest group, association or individual claiming that his or her request for information has been completely or partially rejected by the public authorities.
Complaints have been filed on an annual basis and are anonymised in defense of the personal data of the complaining parties in accordance with the legislation in force.
For each complaint, the portal also provides full access to the text of the decision taken by the Commissioner for the Right to Information to resolve the specific case.
Local government
Zgjidh Institucionin
Year 2017
Search
If you want the Annual Records Record, click below by selecting the corresponding year.
Select Year
GO TO THE
SEARCH
INFORMATION
YOU HAVE NOT RECEIVED AN ANSWER
FORGIVE ME
PUBLICATIONS
Guide who AP is
More
Guidelines on Coordinators
More
Leaflet: How to file a request for information

More
Law on the Right to Information
More
More
SEARCH FOR ASSISTANCE
Emër
Mbiemër
Email
Mesazhi
Leave


Around us
Where to get information
Required information
complaints
Frequently Asked Questions
Frequently Asked Questions
Q-to-common
This section aims to answer some of the most common questions that may arise from anyone investigating this portal or that may be encountered during the implementation of the law "On the Right to Information". Questions are of a substantive nature (such as what we mean by public information) , procedural (where and how to submit information requests) or institutional (the authorities responsible for enforcing the right to information) .
By reading the answers to each of them, you can easily understand how to use the law "On the Right to Information" in your interest and how to orient yourself in relation to institutional procedures for receiving public information or appealing in case of refusal his.
However, if you encounter other questions or complex issues that are not answered in this section you can contact us directly at the following addresses.
The main principles
What is Public Information?
Who are the entities responsible for providing information?
Who needs to make a request for information?
How does information request become?
GO TO THE
SEARCH
YOU HAVE NOT RECEIVED AN ANSWER
FORGIVE ME
PUBLICATIONS
Guide who AP is
More
Guidelines on Coordinators
More
Leaflet: How to file a request for information


Around us
Where to get information
Required information
complaints
Frequently Asked Ques
Photo Gallery
GO TO THE
INSTITUTIONS
SEARCH
INFORMATION
YOU HAVE NOT RECEIVED AN ANSWER
FORGIVE ME
PUBLICATIONS
Guide who AP is
More
Guidelines on Coordinators
More


28 September International Right to Know Day
Good Governance
TRANSPARENCY
REQUEST & RESPONSE
INFORMATION
ACCESS
FREEDOM OF INFORMATION
INFORMATION AND DATA PROTECTION COMMISSIONER

Dr. Tobias Knobloch
Stiftung Neue Verantwortung e. V.

Open Data, Privacy und die Grenzen des Kriteriums Personenbezug

Kürzlich war ich in Athen, um als Mitglied eines Advisory Boards ein großes EU-gefördertes Big-Data-Projekt zu evaluieren. Sieben Mobilitätsbereiche und 13 Pilotprojekte gibt es da. Einige konventionelle Ansätze, die aber dennoch erstmal realisiert werden müssen und am Ende auch zu substanziellen Verbesserungen führen könnten, und richtig tolle Sachen waren dabei. Das Projekt hat einen eigenen Datenmanager, ein eigenes Datenportal, Verfahren zur Sicherung von DSGVO-Compliance usw. Das ist ein wirklich gutes und wichtiges Projekt, um aus der horizontalen, Bereiche-übergreifenden Verknüpfung von Informationen gesellschaftlichen und wirtschaftlichen Gewinn zu ziehen.

Trotzdem oder gerade weil es 2017 ist und ich ein solches Forschungsprojekt evaluiere, fühle ich mich in meiner Überzeugung bezüglich des gesellschaftlichen Stands der Datendebatte bestätigt: Sie krankt an beiden Enden des Spektrums, dem positiv Konstruktiven ebenso wie dem Defensiven. Auf der einen Seite machen wir nicht genug aus Daten und auf der anderen Seite führen wir ein Rückzugsgefecht, das wir nicht gewinnen können. Ich möchte Sie mit meinem Beitrag davon überzeugen, dass wir uns dringend nach alternativen Wegen umsehen müssen, mehr aus unserem Datenreichtum zu machen, ohne dabei in Cyber-Dystopien abzugleiten.

Mit Daten kann man tolle Sachen machen, ja regelrecht die Welt verbessern! In England hat man z.B. durch die Analyse von offenen Daten des britischen Gesundheitssystems herausgefunden, warum am Wochenende mehr Menschen in Krankenhäusern sterben als unter der Woche. Die Erklärung ist ganz trivial: Weil an Wochenenden überproportional häufig junge, unerfahrene Assistenzärzte Dienst haben, während die erfahrenen, diensthöheren Ärzte zu Hause bei ihren Familien sind. Ein anderes Beispiel: Mexiko ist ein Land, das im OECD-Vergleich viel für Bildung ausgibt, aber nur vergleichsweise schlechte Bildungserfolge damit erzielt. Eine Analyse von wiederum offenen Verwaltungsdaten des mexikanischen Bildungswesens hat die schlichten Gründe ans Licht gebracht: Misswirtschaft und Korruption. Etliche Lehrer in den Datensätzen, die auf der Gehaltsliste standen, hatten am 9.9.1919 Geburtstag, manche haben

mehr verdient als der mexikanische Präsident, und es fanden sich Schulen in den Listen mit Adressen, die es gar nicht gibt.

Mehr solcher schönen Beispiele aus dem In- und Ausland, die illustrieren, was man mit Open Government Data zum gesellschaftlichen und wirtschaftlichen Wohl anfangen kann, finden sich auf unserer Website datenwirken.de. Die haben wir eingerichtet, weil immer wieder danach gefragt wird, wozu Open Data eigentlich gut sind, wer sie braucht und nutzt.

Nun lassen sich damit – wie mit allem, bin ich zu sagen geneigt – auch Dinge tun, die wir nicht gutheißen sollten. In Australien haben Wissenschaftler vor einem Jahr etwa gezeigt, dass sie durch Verschneidung von Datensätzen personenbezogene (sowohl Ärzte als Patienten betreffende) Informationen aus Daten extrahieren konnten, die das Gesundheitsministerium veröffentlicht hatte. Und das ist grundsätzlich kein Hexenwerk. Die US-amerikanische Forscherin Latanya Sweeney hat bereits vor vielen Jahren gezeigt, wie leicht sich überschneidende Quasi-Identifikationsmerkmale wie Geschlecht, Geburtsdatum oder Postleitzahl aus unterschiedlichen Datensätzen zur eindeutigen Identifizierung von Personen heranziehen lassen.

Die australische Regierung hat unter dem Eindruck des Skandals, den der oben beschriebene Gesundheitsdatenfall nach sich zog, die De-Anonymisierung von vormals anonymen Daten als meines Wissens erster Staat der Welt unter Strafe gestellt. Schon vorher hatte es in London einen ähnlichen Fall gegeben: Dort sind anonymisierte Daten des Bike-Sharing-Dienstes von ***Transport for London*** mit öffentlich verfügbaren Daten des sozialen Foto-Netztwerks Instagram verschnitten worden, wodurch in den Außenbezirken einzelne Nutzer eindeutig identifiziert und ihre Wege nachgezeichnet werden konnten. Und auch in Großbritannien denkt man inzwischen öffentlich darüber nach, dem Beispiel Australiens zu folgen und im Zuge der Novellierung der Privacy Bill das De-Anonymisieren als Straftatbestand zu definieren.

Das Beste für den Schutz der Privatsphäre ist immer, wenn keine Daten vorliegen. In allen anderen Fällen hat man es stets mit einem Trade-off-Verhältnis zwischen Sicherheit und Nutzbarkeit zu tun. Absolute Sicherheit gibt es nicht, möglich ist lediglich ein guter Schutz, der in vielen denkbaren Szenarien absichert. Stellt sich also die Frage, warum wir mittlerweile überhaupt in allen Bereichen so scharf auf die Auswertung von Daten sind. Die Antwort lautet schlicht: Weil wir auf diese Weise etwas Neues über die Welt, in der wir leben, in Erfahrung bringen und be-

stehende Probleme vielleicht etwas leichter bzw. überhaupt erst lösen können.

Beispielsweise könnten wir im Datenzeitalter irgendwann einen emissionsfreien Individualverkehr ohne die Nachteile des heutigen Verkehrssystems haben. In Kopenhagen etwa nutzt man anonymisierte Standortdaten von 250.000 Verkehrsteilnehmern dazu, um die Verkehrsleitung zu optimieren und dadurch 20 bis 30% Schadstoffemissionen einzusparen. Das ist ungefähr die Menge, die bei uns während des so genannten Dieselgipfels im Sommer 2017 als durch Motorsteuerungsoptimierung bei Dieselfahrzeugen möglicherweise erreichbar diskutiert wurde. Umweltschützer haben das als nicht ausreichend kritisiert, gleichwohl stellt ein solch vorgeschriebenes Software-Update einen Eingriff in das Eigentum vieler Menschen dar. Wie viel einfacher ist es im Vergleich, ohnehin verfügbare Informationen zu Effizienzsteigerungen im Verkehr zu nutzen!

Aber die zeitgenössische Datenverarbeitung bringt auch Erkenntnisse, die zu zweifelhaften Zwecken genutzt werden können. Versicherungen interessieren sich beispielsweise brennend für jede Information, die eine genauere Klassifizierung von Risikogruppen erlaubt. Und sie nutzen dabei ein ökonomisches Anreizsystem, das – wenn man das ohne Restriktionen zulässt und zu Ende denkt – eines Tages möglicherweise in ein Tarifsystem mündet, in dem bestimmte Personen schlicht nicht mehr versicherbar sind, weil die Prämien astronomisch hoch wären. Das liegt einfach daran, dass es sich für jedes Mitglied einer gegenüber der nächst unteren jeweils priviligierten Gruppe lohnt, seine Daten zur Verfügung zu stellen, um nicht zusammen mit dem Risiko-‚Ramsch' gruppiert zu werden. Die Frage ist: Was tun wir mit den Menschen, die am Ende dieses Top-down-Prozesses übrigbleiben, denen keine Versicherung einen bezahlbaren Tarif anbieten mag: Springt der Staat für sie ein, oder verbieten wir oft übermüdeten Schichtarbeitern beispielsweise einfach das Autofahren? Spätestens bei der Übertragung dieses Beispiels auf den Gesundheitsbereich erkennt man, dass hier nicht weniger als der solidarische Sozialstaat zur Disposition steht.

An dieser Stelle wird folgende Einschätzung relevant: Um diese und andere drängende Fragen rund um das Datenthema beantworten zu können, müssen wir die gesamte Datenlandschaft, das gesamte Datenökosystem in den Blick nehmen. Denn nur durch die horizontale Verknüpfung von Informationen über Bereichsgrenzen hinweg werden wir alte Probleme lösen und neue Erfindungen machen können. Allerdings ist es eben auch genau diese Verknüpfung, durch die Gefahrenpotenziale von Datenanalysen aktualisiert werden. Der im Zusammenhang dieser Ta-

gung springende Punkt ist nun, dass das zentrale Datenschutz-Kriterium des Personenbezugs in unserer heutigen Digitalwelt nahezu obsolet geworden ist. Denn mit ausreichend weiteren Informationen im Umkreis, die zunehmend umfangreich zur Verfügung stehen, lassen sich auch anonyme bzw. anonymisierte Daten immer leichter de-anonymisieren und re-personalisieren.

Angesichts dessen müssen wir uns schon fragen, ob der Datenschutz als das bevorzugte Datensteuerungsmodell weiterhin funktioniert. (Natürlich ist der Datenschutz nicht das einzige Datensteuerungsinstrument, das wir haben, wenn wir etwa an die IFG-Familie oder die EU-Datenbankrichtlinie denken. Aber der Datenschutz ist gerade hierzulande doch das zentrale Datensteuerungsmodell unserer Zeit.) Der Punkt ist: Wenn wir die zentralen Grundsätze des Datenschutzes – Einwilligung, Minimierung, Zweckbindung – mit den Kernprinzipien des Datenzeitalters abgleichen, dann braucht man nicht viel Phantasie, um einen gewisses Spannungsverhältnis auszumachen.

Diese Einschätzung wird zumindest von einigen Datenschutzexperten geteilt. Deutschlands erster oberster Datenschutzbeauftragter, Hans Peter Bull, äußert sich in einem aktuellen Aufsatz in der Juristenzeitung etwa skeptisch bezüglich des Grundsatzes der informationellen Selbstbestimmung. Er schreibt: „Die Auslegung und Anwendung des Datenschutzrechts erweist sich zunehmend als problematisch. Eine wesentliche Ursache dieser unbefriedigenden Entwicklung liegt in der verfassungsgerichtlichen Konstruktion eines Rechts auf informationelle Selbstbestimmung und der damit verbundenen abstrakten Vermutung, dass jede Datenverarbeitung ‘riskant‘ sei.“

Ich möchte hier – zumal in diesem Umfeld – keine Debatte über das Grundrecht auf informationelle Selbstbestimmung vom Zaun brechen und schon gar keine Frontlinie gegen den Datenschutz aufmachen. Ich bin froh, dass wir in Deutschland eine starke Datenschutztradition haben, dass wir auf europäischer Ebene die DSGVO haben und dass die EU bei jeder Gelegenheit als ein wertegeleiteter Akteur in der Welt auftritt. (Und aus eben diesem Grund warten kritische Kräfte in den Vereinigten Staaten bereits auf einen Algorithmen-Regulierungsvorstoß seitens der EU, weil sie wissen, dass es einen solchen in den USA so bald nicht geben wird.) Aber wir müssen uns zusätzlich zum Datenschutzinstrumentarium, das wir haben, unbedingt auch die größere Frage stellen, in welcher datengetriebenen Gesellschaft wir eigentlich leben wollen. Längst sind wir eine von Datenanalysen befeuerte Gesellschaft und das wird natürlich weiter zunehmen. Wir müssen eine Skizze entwerfen, wie eine solche

Gesellschaft, die gleichzeitig eine demokratische, gerechte und innovative Gesellschaft ist, aussehen soll. Bisher gibt es eine solche Skizze nicht und der Datenschutz allein wird uns dieses Bild nicht zeichnen.

Mit dieser Auffassung sind wir in der Stiftung Neue Verantwortung glücklicherweise nicht alleine. Die britische Royal Society hat kürzlich eine Studie vorgelegt, mit der sie genau diese Frage zu beantworten versucht: Welche sind die zentralen ethischen und gesellschaftspolitischen Prinzipien für den Informationsfluss in der Datengesellschaft? Ich denke, dass eine Orientierung am Gemeinwohl hier an erster Stelle stehen sollte. Dann sollen natürlich auch Innovationen ermöglicht werden, die wirtschaftliche Gewinne abwerfen. Momentan haben wir allerdings die Situation, dass das Gemeinwohl hintansteht. Wertschöpfung um jeden Preis steht an erster Stelle, während wir versuchen – unter den gegenwärtigen Umständen notwendig vergeblich, wie ich hier zu zeigen versucht habe – die schlimmsten Auswüchse über die Anwendung des Datenschutzrechts einzudämmen.

Neben den britischen Prinzipiengebern haben wir, wenn wir uns nach Instrumenten abseits des traditionellen Datenschutzes umsehen, noch andere Mitstreiter in diesem Feld. Da gibt es beispielsweise einen dänischen Think-and-Do-Tank namens ***Data Ethics***, der Ende 2016 ein bemerkenswertes gleichnamiges Buch über den Trend zu datenethischen Geschäftsmodellen vorgelegt hat. Oder die britische Design-Agentur IF, die den Anspruch des Privacy-by-Design nicht vorderhand technisch versteht, sondern von der User Experience her angeht und den Nutzern von digitalen Diensten über die entsprechende Gestaltung von Benutzeroberflächen die volle Kontrolle über ihre Daten zu geben versucht. Auch diese Herangehensweise ist einen Blick wert, wenn man sich dafür interessiert, wie die Zukunft des Schutzes der Privatsphäre in unserem digitalen Zeitalter ganz praktisch und nicht nur idealer Weise aussehen könnte.

Wir bei der Stiftung Neue Verantwortung sind der Meinung, dass wir zur Bündelung für derlei Bemühungen, um sie ganzheitlich in den Blick zu nehmen, einen neuen Begriff verwenden sollten. Dieser Begriff könnte „Data Governance“ lauten. Im Unternehmenskontext ist er schon gut eingebürgert, um die ganzheitliche Steuerung von Datenflüssen in größeren und mittelgroßen Unternehmen sowie an ihren Außenschnittstellen zu beschreiben. Wir möchten diesen Begriff gerne in die Debatte zur Digitalisierung des öffentlichen Sektors einzuführen und für die gesamtgesellschaftliche Perspektive fruchtbar machen. Auch dafür gibt es Vorbilder: In Österreich ist im Rahmen des nationalen Open-Government-

Vorgehensmodells ein Data-Governance-Modell für die Handhabung von Daten des öffentlichen Sektors entwickelt worden.

Abstrakt verstehen wir unter „Data Governance“ sämtliche Regeln und Rahmenbedingungen, die das Sammeln, Verbreiten, Verarbeiten und Auswerten von Daten anleiten und daraus gezogene Schlussfolgerungen reglementieren. Praktisch fallen rechtliche und verwaltungstechnische Anweisungen darunter ebenso wie ethische Kodizes, technische Normen, wirtschaftliche Selbstverpflichtungen sowie Regeln für den Umgang der Menschen mit ihren eigenen Daten.

In ein Schaubild gebracht (das zum jetzigen Zeitpunkt keinen Anspruch auf Vollständigkeit erhebt) sind aus unserer Sicht mindestens diese Bereiche dabei zu berücksichtigen:

Quelle: eigene Darstellung.

Hier erkennt man schnell, dass die Themen Datenschutz und Open Data jeweils nur einen kleinen Teilbereich ausmachen. Mit anderen Worten: Datenschutz ist heute ein notwendiger, aber nicht hinreichender Teil von Data Governance! Eine derzeit landläufig zu beobachtende Haltung ist jedenfalls nicht zielführend: Die technische und gesellschaftliche Entwicklung verläuft zu schnell, als dass wir die Hände in den Schoß legen und abwarten könnten, was aus der Umsetzung der Datenschutzgrundverordnung (in ihren eher unterbestimmten Teilen) auch auf richterlicher Ebene in den Jahren 2018 folgende werden wird. Auch deshalb gerne die Einladung, unser Projekt „Data Governance“, das gerade gestartet ist und mindestens zwei Jahre laufen wird, zu verfolgen und sich daran zu beteiligen.

Whistleblowing zwischen Datenschutz und Transparenz

u.a. am Beispiel Luxemburg

Thierry LALLEMANG

Vollmitglied der luxemburgischen Datenschutzkommission

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

28 September 2017 – Internationales Symposium – Datenschutz und Informationsfreiheit- Widerspruch oder Ergänzung? – LDA Brandenburg

Inhalt

1. Einleitung
   - Was ist Whistleblowing ?
   - Bedeutung von Whistleblowing
   - Whistleblower setzen sich existentiellen Risiken und Gefahren aus
2. Der rechtliche Schutz von Whistleblowern
   - Internationale und europäische Ebene
   - Artikel 10 (Grundrecht auf freie Meinungsäußerung) der Europäischen Menschenrechtskonvention (EMRK)
3. Schutz von Whistleblowing in Luxemburg
   - Gesetzlicher Rahmen
   - Anwendung der nationalen Gesetzgebung und des Artikel 10 EMRK auf die „LuxLeaks Affäre“
4. Datenschutzrechtliche Aspekte des Whistleblowing

Einleitung (1)

- Kleiner Einblick in die Geschichte:
  - Ein „Löwenmaul“ (Bocca di Leone) am Dogenpalast in Venedig. In der Republik Venedig konnten Denunzianten ihre geheimen Anzeigen in solche „Löwenmäuler“ einwerfen.
  - Der italienische Text lautet übersetzt: „Geheime Denunziationen gegen diejenigen, die Gefallen und Pflichten verheimlichen oder sich im Geheimen absprechen, um deren wahren Gewinn zu verbergen“.

Einleitung (2)

Was sind Whistleblower ?

(im deutschen Sprachraum auch Hinweisgeber, Verpfeifer, Enthüller oder Skandalaufdecker) ?

- Keine einheitliche internationale Definition des Whistleblowers außer auf europäischer Ebene, enthalten in der Empfehlung (2014) 7 des Ministerkomitees des Europarats an die Mitgliedstaaten über den Schutz von Whistleblowern welche auf die Entschließung 1729 (2010) der Parlamentarischen Versammlung des Europarats zurückzuführen ist
  - „jede Person, die im Zusammenhang mit ihrem Arbeitsverhältnis im öffentlichen oder im privaten Sektor Meldungen macht oder Informationen mitteilt über Gefahren oder Nachteile für das öffentliche Interesse“
- Genannte Empfehlung beschränkt also den Schutz des Whistleblowers auf dessen Arbeitsverhältnis
- 6 Kriterien des Europäischen Gerichtshofs für Menschenrechte (EGMR)

Einleitung (3)

Bedeutung von Whistleblowing

- Stärkung von Transparenz und demokratischer Verantwortung
- Unterstützung des Kampfes gegen Korruption und Misswirtschaft
- Frühwarnsystem zur Verhütung von Schäden und zur Aufdeckung von Missständen
- Herbeiführung einer öffentlichen Debatte über den Missstand bzw. Ergreifung geeigneter Maßnahmen zur Vehinderung solcher Missstände für die Zukunft

Einleitung (4)

Whistleblower setzen sich existentiellen Risiken und Gefahren aus

- Diskreditierung / Ächtung / Mobbing
- Disziplinarrechtliche Maßnahmen oder sogar Verlust des Arbeitsplatzes
- Strafrechtliche Verfolgung z.B. wegen Verletzung des Berufsgeheimnisses
- Gesellschaftliche Exklusion

Der rechtliche Schutz von Whistleblowern (1)

Internationale und europäische Ebene

- ILO-Übereinkommen 158 vom 22.06.1982
- OECD-Konvention zur Bestechungsbekämpfung vom 17.12.1997
- Strafrechtsübereinkommen über Korruption vom 27.01.1999 und Zivilrechtsübereinkommen über Korruption vom 04.11.1999 des Europarats vom 27.01.1999
- Arbeiten der Staatengruppe gegen Korruption
- UN-Konvention gegen Korruption vom 31.10,2003 (UNCAC)
- usw.

Der rechtliche Schutz von Whistleblowern (2)

Internationale und europäische Ebene

- **Entschließung 1729 (2010)** der Parlamentarischen Versammlung des Europarats fordert alle Mitgliedstaaten auf, ihre Gesetzgebung betreffend den Schutz von Whistleblowern unter Beachtung einer Reihe von Leitsätzen zu überprüfen und **Empfehlung 2073 (2015)**
- **Empfehlung CM/Rec (2014) 7** des Ministerkomitees des Europarats über den Schutz von Whistleblowern empfiehlt allen Mitgliedstaaten einen normativen, institutionnellen und justiziellen Regelungsrahmen zu schaffen. Das Ministerkomitee erlässt in seiner Empfehlung 29 Grundsätze und betont, dass Whistleblowing eine Form der Ausübung des europäischen Grundrechts auf Meinungsfreiheit darstellt.

Der rechtliche Schutz von Whistleblowern (3)

Internationale und europäische Ebene

- **Richtline (EU) 2016/943** des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den **Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse**) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung

- Vorschlag der Europäischen Kommission für eine Richtline zum Schutz von Whistleblowern für Ende 2017 erwartet

Der rechtliche Schutz von Whistleblowern (4)

Artikel 10 (Grundrecht auf freie Meinungsäußerung) der Europäischen Menschenrechtskonvention (EMRK)

- Schutz durch Art.10 EMRK bei fehlender nationalen Gesetzgebung zum Schutz von Whistleblowern
- In den Rechtssachen Guja/Moldau 12.02.2008 und später Heinisch/Deutschland 21.07.2011 und Bucur und Toma/ Rumänien 08.01.2013 hat der Gerichtshof 6 Grundsätze angeführt, auf die er sich stützt, um festzustellen, ob ein Eingriff in die Ausübung der freien Meinungsäußerung (Artikel 10 EMRK) im Hinblick auf die Handlungen eines Whistleblowers, der öffentlich Informationen mitteilt, „in einer demokratischen Gesellschaft notwendig“ war

Der rechtliche Schutz von Whistleblowern (5)

Artikel 10 der Europäischen Menschenrechtskonvention (EMRK)

- Rechtssprechung des EGMR anhand von 6 Grundsätzen/Kriterien :
  - Die Frage, ob der Person, welche die Informationen mitgeteilt hat, möglicherweise andere Mittel zur Verfügung standen, um Informationen mitzuteilen
  - Das öffentliche Interesse an den mitgeteilten Informationen
  - Die Echtheit der preisgegebenen Informationen
  - Der dem Arbeitgeber zugefügte Schaden
  - Die Gutgläubigkeit der Whistleblower
  - Die Härte der gegen die Person verhängten Sanktion, die Informationen mitgeteilt hat, und ihre Folgen

Schutz von Whistleblowing in Luxemburg (1)

Gesetzlicher Rahmen

- Gesetz vom 13.02.2011 zur Stärkung der Mittel zur Bekämpfung der Korruption → **generelles Whislteblowing-Gesetz** führt spezifische Bestimmungen in das luxemburgische Arbeitsgesetzbuch ein:
  - Anwendung sowohl auf den **öffentlichen** als auch auf den **privaten Sektor**
  - Arbeitsrechtlicher Schutz für Whistleblower oder Zeugen -> **Schutz gegen Repressalien**:
    - **Automatische Nichtigkeit** aller Maßnahmen gegen Whistleblower oder Zeugen z.B. disziplinarische Maßnahmen, Kündigung -> Nichtigkeitsklage
    - **Beweislastumkehr**: Arbeitgeber muß beweisen, daß Maßnahmen zulasten des Arbeitnehmer keinen Zusammenhang mit dessen Whistleblowing hat

Schutz von Whistleblowing in Luxemburg (2)

- Bedingungen für die Anwendung des Whistleblowing-Gesetzes:
  - Whistleblower muß ‘’ **in gutem Glauben** ’’ handeln
  - Meldung muß sich auf folgende Vergehen beziehen: **Korruption, illegale Vorteilsnahme oder Bestechung**
  - **Adressat** der Meldung muß ein **Vorgesetzter** sein oder eine **zuständige Behörde** → Whistleblower nicht geschützt falls er sich an die Presse wendet

- Spezifische **Gesetzgebung über den Finanzsektor**:
  - Einführung eines externen Whistleblowing-Systems für den Finanzsektor bei der Finanzaufsichtsbehörde ‘’CSSF’’
  - Möglichkeit für Arbeitnehmer von Banken und anderen Finanzinstituten Verstöße gegen die Gesetzgebung zur Bekämpfung von Geldwäsche an die Finanzaufsichtsbehörde zu melden
  - Generelles Whistleblowing-Gesetz und Datenschutzvorschriften finden Anwendung

Schutz von Whistleblowing in Luxemburg (3)

- Spezifische Schutzbestimmungen im luxemburgischen **Arbeitsgesetbuch** in den Bereichen:
  - **Sexuelle Belästigung am Arbeitsplatz**
  - **Diskrimination**
  - **Gleichstellung zwischen Mann und Frau**

→ Schutz vor Repressalien im Falle einer Meldung diesbezüglich

→ Beweislastumkehr

Schutz von Whistleblowing in Luxemburg (4)

Anwendung der nationalen Gesetzgebung und des Artikel 10 EMRK auf die „LuxLeaks Affäre“

- Veröffentlichung in der internationalen Presse von 28.000 Seiten mit 548 verbindlichen Steuervorbescheiden (Advance Tax Rulings) von internationalen Konzernen, welche über PricewaterhouseCoopers (PwC) abgeschlossen wurden.
- Whistleblower hatten die vertraulichen Unterlagen missbräuchlich entwendet und an Journalisten weitergegeben
- Strafrechtliche Prozesse in 1. Instanz (Urteil vom 29.06.2016) und 2. Instanz (Urteil vom 15.03.2017) gegen die Whistleblower (ehemalige Arbeitnehmer der Firma PwC) wegen Weitergabe von vertraulichen Informationen

Schutz von Whistleblowing in Luxemburg (5)

Anwendung der nationalen Gesetzgebung und des Artikel 10 EMRK auf die „LuxLeaks Affäre“

- **3 Angeklagte**: Antoine DELTOUR (Hauptangeklagter, ehemaliger PwC-Mitarbeiter), Raphaël David HALET (ehemaliger PwC-Mitarbeiter) und Edouard PERRIN (Journalist); letzterer wurde in beiden Instanzen freigesprochen
- **Hauptanschuldigungen** der Staatsanwaltschaft gegen die Angeklagten: Diebstahl von vertraulichen Dokumenten/Informationen; Verstoß gegen das Berufsgeheimnis und das Geschäftsgeheimnis; Computerbetrug

Schutz von Whistleblowing in Luxemburg (6)

Anwendung der nationalen Gesetzgebung und des Artikel 10 EMRK auf die „LuxLeaks Affäre“

- **1. Instanz**: Verteidigung beruft sich auf das obengenannte generelle Whistleblowing-Gesetz von 2011 und Artikel 10 der EMRK
  - Gericht **erkennt Status als Whistlblower** beider Beschuldigten **an**
  - **Nichtanwendung des Gesetzes von 2011**, also kein Schutz für die Whistleblower, da die Meldung sich nicht auf eines der 3 Vergehen (Korruption, illegale Vorteilsnahme oder Bestechung) bezog und die Meldung nicht an einen Vorgesetzten oder eine zuständige Behörde gerichtet wurde

Schutz von Whistleblowing in Luxemburg (7)

Anwendung der nationalen Gesetzgebung und des Artikel 10 EMRK auf die „LuxLeaks Affäre“

- **Nichtanwendung von Artikel 10 der EMRK**: Nach kurzer Analyse der Interessenabwägung kommt das Gericht zum Entschluß, daß Artikel 10 keine Anwendung findet, weil das öffentliche Interesse der Meldung nicht ausreichend ist und die strafrechtlichen Verfolgung gegen obengenannte Gesetzesvertöße überwiegen
- Strafrechtliche Sanktionen gegen beide Whistleblower:
  - Hauptbeschuldigter Deltour: 12 Monate Freiheitsstrafe auf Bewährung + 1.500 € Geldstrafe
  - Halet: 9 Monate Freiheitsstrafe auf Bewährung + 1.000 € Geldstrafe

Schutz von Whistleblowing in Luxemburg (8)

Anwendung der nationalen Gesetzgebung und des Artikel 10 EMRK auf die „LuxLeaks Affäre“

- **2. Instanz**: Verteidigung beruft sich ausschließlich auf Schutz des Artikel 10 EMRK:
  - Nach umfassender Analyse und Prüfung der 6 obengenannten Grundsätzen des EGMR kommt das Berufungsgericht zum Entschluß, daß Artikel 10 den Beschuldigten zugute kommt, jedoch nur bezüglich der Anchuldigung des Verstoßes gegen das Berufgeheimnis
  - Beschuldigungen des Diebstahls von vertraulichen Dokumenten/Informationen und des Computerbetrugs werden zurückbehalten

Schutz von Whistleblowing in Luxemburg (9)

Anwendung der luxemburgischen Whistleblowing Gesetzgebung und der Rechtsprechung des EGMR anhand der LuxLeaks Affäre

- Strafrechtliche Sanktionen gegen beide Whistleblower:
  - Hauptbeschuldigter Deltour: Herabsetzng der Freiheitsstrafe auf 6 Monate auf Bewährung + 1.500 € Geldstrafe
  - Halet: Keine Freiheitsstrafe, sondern nur noch Geldstrafe von 1.000 €
- **3. Instanz**: Beide beschuldigte Whistleblower sind vor den luxemburgischen Kassationshof gezogen: Verhandlung am 25.11.2017 -> Ausgang ungewiss; Anrufung des EGMR sehr wahrscheinlich
- Reform des luxemburgischen Whistleblowing-Gesetzes ? Ausdehnung des Schutzes von Whistlblowern wenn Meldung an Dritte oder Presse erfolgt ?

Datenschutzrechtliche Aspekte des Whistleblowing (1)

- Die Erhebung und Verarbeitung von personenbezogenen Daten in Whistleblowing-Systemen oder Verfahren zur Meldung von Missständen (im Folgendem: “Meldeverfahren“) unterliegt dem EU- und nationalem Datenschutzrecht
- Europäische Richtlinien durch Artikel 29-Datenschutzgruppe **Stellungnahme 1/2006 (WP 117)** zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen **Rechnungslegung**, **interne Rechnungslegungskontrollen**, **Fragen der Wirtschaftsprüfun**g, **Bekämpfung von Korruption**, **Banken- und Finanzkriminalität** (im Folgenden: Stellungnahme WP 117)

Datenschutzrechtliche Aspekte des Whistleblowing (2)

- Nicht nur Schutz für den Whistleblower sondern auch besonderes Augenmerk auf die Rechte der beschuldigten Person (d.h. Recht auf Mitteilung, Zugang, Berichtigung und Löschung von Daten)
- Stellungnahme WP117 analysiert und bewertet die Vereinbarkeit von Whistleblowing-Systemen mit Datenschutzvorschriften anhand von 8 Punkten:

  1. Rechtmäßigkeit eines Meldeverfahren: nur auf den Rechtsgrundlagen von Artikel 6.1.c. (EU- oder natioanle gesetzliche Verpflichtung) oder Artikel 6.1.f. (überwiegende berechtigte Interessen des Unternehmens) der Datenschutz-Grundverordnung 2016/679 (DSGV)

Datenschutzrechtliche Aspekte des Whistleblowing (3)

2. Grundsätze der Datenqualität und der Verhältnismäßigkeit (Artikel 5 DSGV) → Verhältnismäßigkeitsprüfung:

- Begrenzung der Zahl der anzeigeberechtigten und anzeigbaren Personen
- Förderung von namentlichen Meldungen im Gegensatz zu anonymen Meldungen
- Genauigkeit der verarbeiteten Daten
- Einhaltung strenger Speicherfristen: Löschung innerhalb von 2 Monaten nach Abschluss der Untersuchungen, wenn konsequenzlos

3. Bereitstellung klarer und vollständiger Informationen über das Meldeverfahren

Datenschutzrechtliche Aspekte des Whistleblowing (4)

4. Rechte der beschuldigten Person

- Informationsrechte (Artikel 14 DSGV)
- Rechte auf Auskunft, Berichtigung und Löschung (Artikel 15-17 DSGV)

5. Sicherheit der verarbeiteten Daten :

- Materielle Sicherheitsmaßnahmen (Artikel 32 DSGV)
- Vertraulichkeit von Meldungen

6. Management von Meldeverfahren:

- Spezifische interne Einheit für das Management des Whistleblowing-Systems
- Möglichkeit externe Dienstleister als Auftragsverarbeiter heranzuziehen

Datenschutzrechtliche Aspekte des Whistleblowing (5)

7. Fragen im Zusammenhang mit der internationalen Übermittlung von Daten (Artikel 44-49 DSGV)

8. Vorabmeldung / Vorabkontrolle des Whistleblowing-Systems hängt im Moment noch von den nationale Gesetzgebungen der Mitgliedstaaten ab (Anwendung Richtlinie 95/46/EG)

→ Nach den Bestimmungen der **DSGV** werden Datenverarbeitungen bezüglich Whistleblowing-Systemen der Pflicht, eines jeden Verantwortlichen ein Verzeichnis von Verarbeitungstätigkeiten zu führen (Artikel 30 DSGV) und eventuell der Durchführung einer Datenschutz-Folgeabschätzung (Artikel 35 DSGV) unterliegen. Beim Einführen solcher Systeme sollten außerdem die Bestimmungen des Artikel 25 DSGV berücksichtigt wedren d.h. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung

Schlussvolgerung

- Viele Unternehmen scheinen noch nicht bereit oder Reif für das Einsetzen von Whistleblowing-Systemen

.

- Arbeitgeber die Whistleblowing-Systeme eingeführt haben sind selbst oft nicht bereit Meldungen von Missständen in ihren Betrieben zu hören, auch wenn tatsächliche Vorteile von Whistleblowing nicht von der Hand zu weisen sind
- Von seiten der Politik bzw. der europäischen Kommission besteht Handlungsbedarf zur Schaffung eines ausgeglichenen und umfassenden gesetzlichen Rahmens innerhalb der EU
- Und trotzdem: auch mit gesetzlichen Regelungen bleibt die Gefahr der Beeinträchtigung von Whistleblowern. Unerlässlich ist es sich auch für deren Akzeptanz in der Gesellschaft einzusetzen

Literatur und Fundstellen

- 29-Datenschutzgruppe Stellungnahme 1/2006 (WP 117, 01.02.2006) zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität;
- Empfehlung CM/Rec(2014)7 des Ministerkomitees des Europarats über den Schutz von Whistleblowern empfiehlt allen Mitgliedstaaten einen normativen, institutionnellen und justiziellen Regelungsrahmen zu schaffen. Das Ministerkomitee erlässt in seiner Empfehlung 29 Grundsätze und betont, dass Whistleblowing eine Form der Ausübung des europäischen Grundrechts auf Meinungsfreiheit darstellt + Erläuternder Bericht zur Empfehlung;
- Digma, Zeitschrift für Datenschutz und Informationssicherheit, Heft 1, März 2016, Schulthess
- Internationalrechtliche Regulierung des Whistlblowing- Anpassungsbedarf im deutschen Recht, September 2015, Prof. Dr. Andreas Fischer-Lescano, Universität Bremen;
- Whislteblowing-Hotlines: Firmenintern Warnysteme und Beschäftigtendatenschutz, Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz“ des Düsseldorfer Kreises;
- „Whistleblowing: état des lieux et conseils pratiques“, Di Stefano - Moyse, avocats à la Cour;
- „Lanceurs d‘alerte: que dit la CEDH ?“, Hélène Weydert, Avocat à la Cour;
- „Le lanceur d‘alerte interne: une personne concernée par le traitement de ses données à caractère personnel, mais également par son avenir professionnel…“ , Fanny Coton, Jean-François Henrotte, avocats;

Vielen Dank für Ihre Aufmerksamkeit !

Thierry LALLEMANG
Commission nationale pour la protection des données

Commission nationale pour la protection des données

1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette (Belval)
261060-1
www.cnpd.lu
info@cnpd.lu

Xiaowei Chen
Bundeskanzler-Stipendium (Alexander von Humboldt Stiftung) / Open Knowledge Foundation Deutschland e. V.

Personal Data and The Principle of Public Access in Sweden: Too Much Transparency in the Digital Age?

As a German Chancellor scholar from China, I was invited this May and June to visit Stockholm and research on transparency in Sweden. During the eight weeks, I talked to professors, layers, judges, journalists, highly-ranked public servants etc. I was amused by the transparent tradition in this country and also got very impressed by the current circumstance, especially as I learned that any question to the government would be answered within two days otherwise people could already complain, I literally envied Swedish citizen who just took it for granted.

I also envied them when asking about salaries of government officers- or public servant, as the Swedish would call them. Since Xi Jinping was elected Chinese President in 2012, Chinese central government has spent years trying to make income and wealth of public servants transparent in the anti-corruption campaign yet failed to make significant progresses. With the expectation of hearing exciting and valuable experiences, I discussed this matter with many Swedish people. A 25 years old Swedish man gave a most representative answer: “All salaries in public sector are open and therefore not interesting for us.” True. Swedish National Mediation Office publishes the figures each year, you will find everything you need on their website.

This kind of transparency does not invade personal privacy. In most countries, anyone in public sector is aware that his income would be transparent. Yet to draw a question mark for China, maybe also for some other countries like USA: If someone becomes a public servant, does he give up automatically the right of keep his wealth confidential? It is not only salary I’m talking about, but also his tax record before entering the government, as well as the benefits he and his family receives during the duty.

In China or Germany, I don´t think there is a general way to find out how many houses and cars your neighbour holds, or how much tax he pays each year. Yet in Sweden, you can easily start digging if you know his name. And no, he doesn’t have to be a public servant.

On Website www.hitta.se, search a name and you will get his home address, street view, telephone number, birthday. We can also send him flowers on his birthday through a click on www.hitta.se.

And more information about this neighbourhood followed:

A list of names who are also registered in this address, another list of names who moved in and moved out from the neighbourhood, average price of the houses, which cars are mostly driven in this living block, and of course, the average income.

You don't need to be a skilled hacker, and don't even need to pay anything for this information. However, if you demand an ID protection from hitta.se to keep your personal information confidential, it costs 99 kr (10 Euro) per month.

This website was founded in 2004, is now one of the most widely used websites in Sweden. According to its homepage, over 3 million individuals are searched each week. Guess what's the population in Sweden? 9.9 Million.

Well, with all these information gathered, we are unfortunately still a few steps away from getting to know the income of this particular person. In order to request a tax record, we have to provide an essential factor to the Tax Office: social security number of a Swedish resident.

It is time to move to a more powerful website: www.ratsit.se.

Search the same name, we now get more detailed information: whether he owns or rents the apartment, which cars he drive. And if you register, his whole complete social security number is no secrets anymore! And now we can turn to the Swedish Tax Agency and ask about his tax record and income- the request is free of charge and Raj himself would know nothing about this.

Oh wait, Ratsit.se suggests another possibility: "The Swedish Tax Agency has approved 8 413 154 income declarations and the catalog is newly updated. RAJ is included in this catalog." Seems we need to buy a Ratsit Directory.

This is a book that includes income details of all Swedish residents over the age of 18: Name, address, age, salary, income from capital... Every-

thing. Price? 249 kr (25 Euro). The only shortage: This is not an E-book, that could be easily transformed into a nice Excel document.

My friend Raj from Indian was not pleased to find out how convenient it was to get his personal information, he took this as an invasion of his privacy. But he also benefits from the transparency: His IT company uses hitta and ratsit to find telephone number of important potential customers.

After finding this, I couldn't stop worrying about all kinds of possible frauds. Similar Stories have been reported in Chinese media, some lost their savings, some lost their apartments. Last year, a young girl from a poor family passed exams and entered college successfully, her proud parents borrowed money from the whole village for her study fee. A con man collected her personal information illegally and pretended to be a donator from her college, asking her to pay a deposit for a scholarship. The innocent freshman lost all her money in the scam, was fully desperate, and then committed suicide.

Just imagine, how simple it is to fake an ID in Sweden if I plan to do bad things, and how precise bad guys can target their goals. If a team digitalize the Ratsit Directory, experts could analyze the economic conditions of residents in a building, in an election zone, in a city and in the whole country, not many secrets could be hold. I shared my concerns with many Swedish friends, and ask what they feel to share all these information online. To my huge surprise, almost all Swedish don't see problems in this. On the contrary, many are rather proud.

During my last week in Stockholm, I met Ola Sigvardsson, the press ombudsman in Sweden. Because one fair judgement of his in 2012 defended the right of an immigrant, a bunch of extreme-left Swedish men decided to protest against him. Not in front his office, but in front of his home. They found Ola's address from hitta.se and pulled pig blood all over the entrance of his apartment. Neighbors were not pleased, police got involved, and Ola's wife felt angry and upset.

On his position I would definitely apply for an ID protection. But Ola chose to stay transparent: "Staying on hitta.se is one of my ways to keep and defend openness and transparency." He believes, transparency is a way to build a society where people feel secure, where rumors don't grow beneath the surface. If you start reducing transparency, you start building walls within the society, which only makes problems get worse. Ola refuses to build walls around him.

A famous journalist said he could not image working without personal data banks, he found it great that Swedish society was surprisingly transparent for me.

A highly ranked government officer of Swedish Parliament felt a little troubled when her work mails sometimes delivered to her home, but would be glad to let her personal information stay available.

A successful businessman said he wouldn't employ anyone who is not to be found on hitta or ratsit.

A student majored in journalism found it pretty fair. She goes with the principle: Everyone can find anyone, nobody hides.

Only foreigners in Sweden seem to feel uncomfortable when they know how open the society is. In Sweden, I actually sensed a great amount of trust. People trust each other, supermarket trust the customers, citizen trust their government – well, at least much more than German or Chinese trust theirs.

Trust is such a rare thing in China nowadays. A few years ago, an old man fell on the floor. A passer-by tried to help, but got himself in trouble of being accused of knocking the old man down at the first place. "If it wasn't you, why bother to help?" So said the son of the old man. If there wasn't monitor, the passer-by would have to pay thousands euros. And yes, when other old men fell later, nobody dared to help without taking a picture of the accident first.

For thousands of years, China has called itself state of ceremonies (礼仪之邦), but the reality could sometimes be very ironic. Some regulation of the government are impressive merely on paper, Chinese newspaper tells half truth, patients bride their doctors for better treatment, and if somebody helps an old man who fell on the floor, his behavior would be praised in the news because this has become not a normal thing. I have to keep asking, when and why did most Chinese stop trusting our systems, and our own people. This was one important reason why I got interested in transparency in other countries, hoping that transparency might provide a solution to some political and ethical problems in my homeland.

There was a time that I felt some Swedish were some kind of naive in believing the rest of the world wouldn´t abuse their personal information,

and I’m sure some of them thought I was being paranoid. When Ola Sigvardsson said determined that he refused to build a wall in Swedish Society, I got to understand some Swedish spirit at the very moment.

I still treasure trust as a rare thing. It is therefore extremely valuable, and maybe more fragile than we think. A terror attack in Stockholm could have destroyed secure feelings of hundreds Swedish citizens. Ten years of culture revolution might have destroyed the trust build over thousands of years in the Chinese Society.

Transparency and openness provides basic stones to build trust, could but also be abused to destroy it. The freedom of information is written since 251 years in Swedish constitution, but is the law also prepared for the digital age? Sweden must be prepared to these challenges.