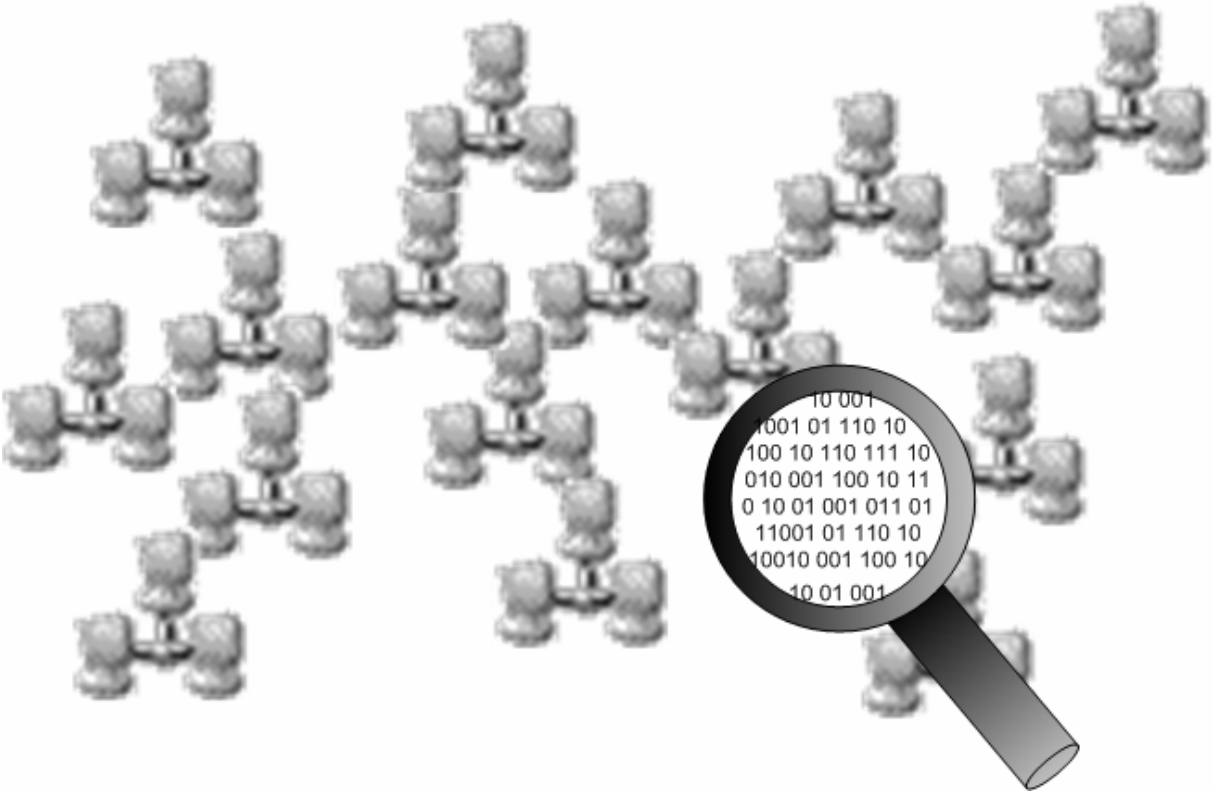


Information Systems Assurance and Control Guideline

for Verifing Compliance with Personal Data Protection Act

An UODO Survival Kit

ODOSI Project Team
Mirosław Błaszczak
Piotr Dzwonkowski
Joanna Karczewska
Sebastian Łataś

Version 2.1
Warsaw, December 2007

Disclaimer:

The ODOSI Project Team has created this document (the "Guideline") primarily as an educational resource for professionals. The ODOSI Project Team makes no claim that use of any of the Guideline will assure a successful outcome. The Guideline should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the assurance and control professional should apply his or her own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Guideline Version

So far the ODOSI Project Team has published the following versions of the Guideline:

version 1.0 PL - in March 2005,
version 1.1 PL & EN - in April 2005,
version 2.0 PL - in December 2006
version 2.1 PL - in October 2007.

Changes in this version were based on suggestions and comments from users of the Guideline and include an upgrade of the Guideline to version 4.1 of the COBIT framework.

Comments:

The ODOSI Project Team welcomes any input concerning the Guideline. Please send your comments to:

Mirosław Błaszczak m.blaszczak@vip.wp.pl
Piotr Dzwonkowski piotr.dzwonkowski@gmail.com
Joanna Karczewska j.karczewska@poczta.onet.pl
Sebastian Łataś sebastian.latas.s@gmail.com

December 2007

Warsaw, Poland

TABLE OF CONTENTS

Everyone shall have the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life

Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law

The Constitution of the Republic of Poland

1. BACKGROUND

1.1. Introduction

In today's highly formalized and computerized world our personal data are collected by countless firms and public institutions. Our personal data are stored in electronic form, which makes their processing and distribution much easier and faster. There is no way we can personally control our personal data and prevent their use contrary to the purpose for which they are collected. Therefore we have the right to demand from those who have our permission to collect and process our personal data that they ensure protection of that data. We should be asking the following question:

„Are our personal data adequately protected?"

The executive management of firms and public institutions should realize that personal data collected by their organisations are stored in innumerable forms in many different places and that many employees have access to them. Personal data are stored in electronic form, because this makes their processing and distribution much easier and faster. However this creates specific threats and forces organisations to implement additional security measures, so that personal data are collected and processed in compliance with Polish laws and regulations. Firms, public institutions and associations (practically every organisation processes personal data) should be asking the following questions:

„Are we processing personal data in compliance with all legal requirements?"

„Are we adequately protecting the personal data that we are processing?"

1.2. Laws and Regulations

The following Polish laws and regulations define legal principles of the protection of personal data:

- The Constitution of the Republic of Poland
- Act of August 29th, 1997 on the Protection of Personal Data (Journal of Laws of 2002 No 101, item 926 with later amendments) – referred to as „UODO",
- Regulation by MSWiA dated April 29th, 2004 (Journal of Laws of 2004 No 100, item 1024) about the scope of documentation as well as basic technical and organisational conditions which should be fulfilled by devices and computer systems used in processing personal data – referred to as „Regulation". The Regulation became effective on November 1st, 2004,

and in Europe:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,
- Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, dated January 28th, 1981.

In particular cases other local and international laws and regulations may also apply.

1.3. Need for Guideline

Directive 95/46/EC in item 61 of the Recitals states:

" Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation."

There are many such publications available in bookstores and on the Internet. Developed by different entities and organisations, they address legal issues relating to the protection of personal data. However there is a distinct lack of publications that discuss issues concerning the protection of personal data in information systems. For that reason members of the ODOSI Project Team decided to develop an IS Audit and Control Guideline to help ensure compliance, security and control of the processing of personal data in information systems.

The Guideline does not include topics strictly concerned with the protection of classified information, as defined in the Act on the Protection of Classified Information (Journal of Laws of 2001 No 22, item 241).

1.4. Target Audience

The Guideline is intended for all those interested in assuring compliance of information systems with UODO. The table below provides a list of target groups and their roles:

	Target Group	Role
1.	Personal Data Controller / Executive Management	Is accountable for the protection of personal data. As stated in UODO Article 7, it means a body, an organisational unit, an establishment or a person referred to in Article 3, who decides on the purposes and means of the processing of personal data.
2.	Administrator of Information Security (called ABI)	Supervises the compliance with security principles, appointed by the controller, unless the Personal Data Controller performs these activities by himself (as stated in UODO Article 36).
3.	Managing Administrator	Is responsible for the processing of personal data in a given area.
4.	Data Custodian (e.g. System/Application/Server Administrator) – IT specialist	Performs ongoing activities concerned with the protection of personal data in a given system or application.
5.	Data Subject	Has the right to control the processing of his/her personal data contained in the filing systems (as stated in UODO Chapter 4).
6.	Other Subject authorized to process personal data (outsourcing)	Prior to processing the data, the Other Subject shall be obliged to provide security measures protecting the data filing system, as defined in UODO Articles 36–39, and to meet the requirements specified in the provisions referred to in UODO Article 39a.
7.	IS Auditor	Verifies compliance of personal data processing with UODO.

	Target Group	Role
8.	GIODO Inspector	Performs inspections of any devices, data carriers, and computer systems used for data processing (as stated in UODO Article 14).

1.5. Reference to ISACA® and COBIT®

With more than 65,000 members in 140 countries, **ISACA**® is the leading worldwide organisation for professionals involved in IT Governance, control, security and audit of information systems. Formalized in 1969. The ODOSI Project Team members are all members of ISACA.

IT Governance Institute® (ITGI) was established by ISACA in 1998 to assist enterprise leaders in aligning IT to business needs and providing measurable benefits from information technology while appropriately managing IT resources and risks. ITGI conducts original research on IT governance and related topics. ITGI develops publications designed for professionals working in an ever-changing IT environment.

COBIT® (Control Objectives for Information and Related Technology), designed and updated by ISACA® and ITGI®, is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. It enables clear policy development and good practice for IT control throughout organizations. The latest version emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework. Professionals from all over the world, including Poland, take part in ISACA and ITGI projects.

1.5.1 Information criteria

To satisfy business objectives, information needs to conform to certain control criteria, which COBIT refers to as business requirements for information. These are: effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability. For information security two basic criteria apply: confidentiality and integrity. As defined in ISACA® documents, **accountability** means the ability to establish, who authorises a given activity or event.

As stated in the Regulation, the following criteria: confidentiality, integrity and accountability apply when processing personal data. **Accountability** means the ability to map a given activity or event back to the responsible party in information systems and devices used to process personal data.

1.6. Linkage to other Standards and Guidelines

In matters concerning the protection of data and information systems we recommend referring to other well-known practices and guidelines described in the publications listed below.

1.6.1 COBIT publications

IT Governance Institute® has published several documents concerning data security, including:

- CobiT Security Baseline – An Information Security Survival Kit, 2nd Edition [5]
  – discusses IT security issues in a way that is simple to follow for the home user, the employee of a small or medium enterprise, as well as for the executives and board members of a large organisation,
- COBIT Mapping Overview of International IT Guidance, 2nd Edition [6]
  – presents a comparison of 14 different international standards and guidance for IT control and IT security,
- CobiT Mapping: Mapping of ISO/IEC 17799:2005 With CobiT 4.0 [7]
  – presents relations between the processes and control objectives defined in the CobiT framework and the best practices described in the well-known international standard.

1.6.2 Information Security Standards

The following well-known and widely used standards can be applied to provide confidentiality, integrity and availability of data in information systems:

- ISO/IEC 27001:2005,
- ISO/IEC 27002:2005,
- ISO/IEC 17799:2005,
- Polish standard PN-ISO/IEC 17799:2007,
- Polish standard PN-ISO/IEC-27001:2007.

1.6.3 GIODO Guidelines

GIODO has published three documents for data administrators, developed by the IT Department (available on their website):

- Guidelines for the design and implementation of a security policy [10],
- Recommendations on developing an instruction for managing information systems processing personal data, including specific requirements for information security [11],
- Requirements for the structures of personal data filing systems and the functionality of the applications used for their management [12].

1.7. Reference to Privacy

The „Electronic Dictionary of the Polish Language" published by PWN, defines privacy as:

„Private, personal life and matters, the feeling of security in one's own home; the right to intimacy, protected from interference by strangers."

Privacy is also referred to in Article 47 of the Polish Constitution:

„Everyone shall have the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life."

Encyclopoedia Britannica gives a similar definition of privacy:

"Right of a person to be free from intrusion into matters of a personal nature.
A person's right to privacy may be overcome by a compelling state interest. In tort law, privacy is a right not to have one's intimate life and affairs exposed to public view or otherwise invaded. Less broad protections of privacy are afforded public officials and others defined by law as "public figures" (e.g., movie stars)."

Wikipedia includes probably the most intuitive definition of privacy:

„It is the ability of an individual or group to keep their lives and personal affairs out of public view."

It is considered, that the right to the protection of personal information comes from the right to privacy. Appropriate statements were comprised in Article 51 of the Polish Constitution:

„1. No one may be obliged, except on the basis of statute, to disclose information concerning his person.
2. Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law.
3. Everyone shall have a right of access to official documents and data collections concerning himself. Limitations upon such rights may be established by statute.
4. Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute.
5. Principles and procedures for collection of and access to information shall be specified by statute."

UODO constitutes a legal expansion of this Article.

We would like to point out, that in our contemporary world that widely incorporates information systems, the meaning of the term “privacy” is often narrowed to matters regarding information concerning an individual. A good example is the IS Audit Guideline Privacy [9] published by ISACA, where the term „privacy” is used to describe „data privacy”:

“1.6.1 Privacy means adherence to trust and obligation in relation to any information relating to an identified or identifiable individual (data subject). Management is responsible to comply with privacy in accordance with its privacy policy or applicable privacy laws and regulations.”

1.8. ODOSI Project Team

The inspiration for the ODOSI Project came from the IS Audit Guideline Privacy published by ISACA in 2004 [9].

The ODOSI Project team consists of four members of ISACA Warsaw Chapter:

- Mirosław Błaszczak, CISA,
- Piotr Dzwonkowski, CISA, CISM,
- Joanna Karczewska, CISA,
- Sebastian Łataś, CISA, CISM.

Version 1.0 of the Guideline was made public for consultations in March 2005. The received comments and changes were added to versions 1.1 and 2.0. The current version 2.1 includes comments received during the past 2 years and an upgrade to version 4.1 of the COBIT framework.

1.9. Reference to e-PRODAT

Version 1.1 of the Guideline qualified for the „Third Edition of the Prize to the European Data Protection Best Practices in Public Administrations” organised by The Data Protection Agency of the Region of Madrid (in Spanish: Agencia de Protección de Datos de la Comunidad de Madrid - APDCM). The Guideline was presented during the international seminar that took place in Madrid on December 12th, 2006.

APDCM is also the leader of the European project "e-PRODAT: e-Government and the Protection of Personal Data in European Regions and Cities", co-finansed by the European Union as part of the INTERREG IIIC Initiative. The Project has three main goals:

- the exchange of knowledge and experiences related to personal data protection in public bodies belonging to different European countries.
- to create an Internet based “European e-Government data protection observatory”, for the permanent assessment on the accomplishment with European data protection laws and principles and the awareness of data protection issues among European citizens,
- identifying best data protection practices already in place for e-Government or other public bodies services, and building recommendations for increasing data protection standards in the public sector.

Information abort the e-PRODAT project and the created Observatory are available at:

www.eprodat.org

We also recommend the following website:

www.dataprotectionreview.eu

edited by APDCM and dedicated to the protection of personal data In the European Union.

2. GUIDELINE

2.1. Use of the Guideline

The Guideline can be used by persons concerned with the protection of personal data independent of their level of knowledge and the progression of work.

	Responsibilities	Recommended actions:
1.	Persons, who are just beginning to be involved in the protection of personal data in information systems	I. Read UODO and the Regulation (together with commentaries if possible) II. Ask questions from the check-list to determine to what extent UODO and the Regulation apply in the enterprise III. Use the mapping and appropriate Control Practices of the COBIT Framework to determine what, why and how to implement in information systems to ensure compliance with UODO
2.	Persons, who have already implemented measures of protection of personal data in information systems	I. Check whether UODO or the Regulation were amended and read the changes II. Ask all questions on the check-list to determine the level of compliance with UODO and the Regulation III. Use the mapping and appropriate Management Guidelines of the COBIT Framework to determine: • key controls, • key metrics, • roles and responsibilities (RACI) for the related activities, • activity goals, process goals and IT goals for the relevant IT processes
3.	Persons in charge of total management of an enterprise or organisation (Personal Data Controllers)	I. Read UODO and the Regulation (together with commentaries if possible) II. Obtain answers to questions listed in the first column of the check-list III. Use the mapping and the Management Guidelines of the COBIT Framework to determine the maturity level of the relevant IT processes
4.	Persons, who want to audit / verify compliance with UODO	I. Read UODO and the Regulation (together with commentaries if possible) II. Obtain answers from persons responsible as defined in column headings of the checklist table to determine the level of compliance with UODO and the Regulation III. Use the mapping and the Assurance Guide of the COBIT Framework to verify compliance of information systems with UODO

2.2. Check-lists

The table below comprises check-lists with questions referring to specific articles of UODO. Answers to these questions can help identify, implement and improve controls preventing violation of the security of personal data as well as verify compliance of personal data processing with UODO. These questions are generic, which means that not all questions will be applicable in every organisation. Stakeholders must decide whether a particular question is applicable, depending on the size, culture, structure and maturity level of their organisation.

Three specific target groups were defined:

1. **Personal Data Controller (ADO)** – is accountable for the protection of personal data. As stated in UODO Article 7, it means a body, an organisational unit, an establishment or a person referred to in Article 3, who decides on the purposes and means of the processing of personal data.

   Based on personal experience the ODOSI team members find that in large and medium organisations it is important to identify persons responsible for personal data processing in specific areas (e.g. marketing director, CFO, HR manager). We called these persons the **Managing Administrator**.
2. **Administrator of Information Security (ABI)** –supervises the compliance with security principles, appointed by the controller, unless the controller performs these activities by himself (as stated in UODO Article 36),
3. **Data Custodian** (e.g. System/Application/Server Administrator) – performs ongoing activities concerned with the protection of personal data in a given system or application.

The internal control and external audits are not required by UODO. However these activities are recommended as a good practice and are implemented in many organisations. Based on personal experience the ODOSI team members decided to include questions referring to these activities on the check-lists.

The names of groups of questions refer to articles/chapters of UODO and the Regulation.

No	Personal Data Controller or Managing Administrator	Administrator of Information Security (ABI)	Data Custodian (e.g. System/Application/Server)
PERSONAL DATA FILING SYSTEMS			
Applicability (art. 2, 3, 3a, 6, 40)			
1	Is UODO applicable in our company/organization?	To what extent is UODO applicable in our company/organization? Are there any exceptions?	Have I been informed that UODO is applicable to data filing systems that I administer?
2	What personal data, as defined in UODO, is processed by our company?	What personal data, as defined in UODO, is processed by our company in data filing systems/files?	What personal data, as defined in UODO, is processed in the data filing systems that I administer?
3	Do we also (only) collect/process data files prepared ad hoc?	Which of the data filing systems are data files prepared ad hoc?	Are the data filing systems that I administer data files prepared ad hoc, for technical or training purposes?
4	Which data filing systems contain personal data?	Which of the company's data filing systems contain personal data as defined in UODO?	Which of the data filling systems that I administer process personal data?
5	Do data filing systems contain sensitive data?	Which data filing systems contain sensitive data?	Do data filing systems that I administer contain sensitive data?
6	Is there a list of these data filing systems? Where is it stored?	What is the format of the list of data filing systems? Where is it stored and how is it secured?	Do I prepare and update a list of data system files that I administer?
7	Is the list mentioned above complete and up-to-date?	What assurance is there that the list mentioned above is complete and up-to-date? How are entries logged?	When did I last update the list of data filing systems?
8	Do the data filing systems have to be registered at GIODO?	Which data filing systems have to be registered at GIODO? What is the procedure for preparing GIODO registration forms?	Do the data filing systems that I administer have to be registered at GIODO?
9	Have data filing systems due for registration been registered?	How is the documentation confirming registration at GIODO maintained?	Have data filing systems that I administer been registered at GIODO?
10	Is personal data processed in the company's information systems?	Is personal data processed in the company's information systems? In which systems? Is it personal data as defined in UODO?	Is personal data processed in the systems that I administer?
Roles and responsibilities (art. 7, 36, 37, 33, 34)			
11	Which member of the management is responsible for the protection of personal data?	Which member of the management supervises my work as ABI?	Which member of the management is responsible for the protection of personal data?

No	Personal Data Controller or Managing Administrator	Administrator of Information Security (ABI)	Data Custodian (e.g. System/Application/Server)
12	Who is accountable for personal data processing in the controlling organization?	Do I known the contact person in charge of personal data processing in the controlling organization?	Is the person (from the controlling organisation) with granted admin rights known and formally authorized to process personal data?
13	Who is accountable for personal data process in the controlled organization?	Am I responsible for personal data processing in the controlled organization?	Are admin rights of administrator(s) from the controlled organization known and verified?
14	Who is officially appointed as ABI?	When was I appointed as ABI?	Who is appointed as ABI in our company?
15	Are ABI's responsibilities formally defined?	Have I received and accepted my responsibilities as ABI?	Do I know the responsibilities and authorizations of ABI concerning the data filing systems that I administer?
16	How does ABI supervise the rules of personal data protection?	How do I supervise technical and organizational measures which protect personal data against: unauthorized access, unauthorized removal, processing not compliant with UODO, unauthorized change, loss or damage?	How are implemented technical and organizational measures protecting personal data against: unauthorized access, removal, change, loss or damage?
17	Have administrators been appointed to systems /applications processing personal data?	Is there a list of data filing system administrators? Is it up-to-date and complete?	Do I know my responsibilities as administrator of a system/application containing or processing personal data?
18	Who is authorized to process personal data?	What is the procedure for authorizing staff to process personal data? Who is responsible for preparing and storing the documentation?	Do users having access /processing personal data in data filing systems that I administer have proper authorization?
19	Who is authorized to provide information about personal data processed by the company?	Who is authorized to provide information about personal data processed by the company? How was he authorized?	Who is authorized to provide information about personal data processed in data filing systems that I administer? How was he authorized?
PROCESSING OF PERSONAL DATA			
Grounds for processing (Chapter 3)			
20	What is the purpose of personal data processing?	What is the purpose of personal data processing? Who authorized it? Do the reasons change?	Have I been informed about the purpose of personal data processing in the data filing systems that I administer?
21	What is the scope of personal data processing?	What is the scope of processing for each data filing system?	What is the scope of processing for each data filing system that I administer?
22	Is consent for personal data processing required from data subjects?	For which data filing systems is consent for processing required from data subjects?	Is consent from data subjects required for processing data filing systems that I administer?

No	Personal Data Controller or Managing Administrator	Administrator of Information Security (ABI)	Data Custodian (e.g. System/Application/Server)
23	Do we have the consents of data subjects for personal data processing?	What is the format of the consents? Where are they stored? Are they in accordance with the established and real scope and purpose?	
24	In what form are the consents stored? Where?	Are consents for personal data processing stored and archived in a way that allows easy access to them?	Are consents required for processing data filing systems that I administer?
25	Was personal data processed by our company obtained by transfer from a third-party?	Which data filing systems are processed based on transfer from a third-party?	Were data filing systems that I administer obtained by transfer from a third-party?
26	Have data subjects been informed as required by law?	How have data subjects been informed as required by law?	
27	Are data filing systems properly protected?	Are security criteria required by UODO in place relating to data filing systems?	Are security criteria required by UODO in place relating to data filing systems that I administer?
Principles of processing (Chapter 3)			
28	Is personal data complete and accurate?	How do we ensure that personal data processed by the company is complete and accurate?	Is personal data processed in data filing systems that I administer complete and accurate?
29	Does personal data processing correspond to the stated purpose and scope?	How do we ensure that personal data processing corresponds to the stated purpose and scope?	Does personal data processing in data filing systems that I administer correspond to the stated purpose and scope?
30	How do we ensure that the final decision in an individual case of the data subject is not just the result of data processing in the information system?	Do we have information systems in which the final decision of an individual case of the data subject is just the result of data processing?	Am I sure that in systems that I administer the final decision of an individual case of the data subject is not just the result of data processing?
31	In the case of sensitive data processing, are requirements from art. 27.2 met?	Is the fulfillment of special requirements concerning sensitive data processing verified? How? What are these requirements?	Are data filing systems which I administer processing sensitive data?
32	If internal sequence numbers are used, are they assigned any hidden meaning (art.28)?	If internal sequence numbers are used in all filing systems, are they assigned any hidden meaning?	If internal sequence numbers are used in data filing systems which I administer, are they assigned any hidden meaning?

No	Personal Data Controller or Managing Administrator	Administrator of Information Security (ABI)	Data Custodian (e.g. System/Application/Server)
Disclosure of data (art.29, 30, 35)			
33	Are there any procedures concerning disclosure of personal data (not to a data filing system)?	What are the procedures concerning disclosure of personal data?	Are there any controls concerning disclosure of personal data implemented in data filing systems that I administer?
34	Are procedures concerning disclosure of personal data verified?	How are procedures concerning disclosure of personal data verified?	Are features for logging any disclosure of personal data implemented in data filing systems that I administer?
35	Are there any procedures concerning refusal to disclose personal data (not to a data filing system)?	What are the procedures concerning refusal to disclose personal data?	
Transfer of data (art. 38)			
36	Do we transfer data filing systems that the company administers to a third party?	Which data filing systems are transferred to a third party? Are there procedures concerning transfer? Are scopes of data transferred defined?	Are data filing systems that I administer transferred to a third party? Are transfer formats defined? Are scopes of data transferred defined?
37	Are logs of transfers available?	Do logs of transfers include information about scopes, file names, dates and recipients?	Do I take part in the process of data transfer and do I have a transfer log?
38	Do we have the consent of data subjects for data transfer?	How are the consents of data subjects for data transfer stored?	
Authorisation of processing (art. 31)			
39	Is processing of personal data that the company administers outsourced?	What processing of data filing systems (or parts) is outsourced?	Are data filing systems that I administer outsourced?
40	Are the contracts for outsourcing signed?	Are the contracts for all outsourced processing signed?	Do I know the contract clauses defining rules for outsourcing processing of personal data that I administer?
41	Are the procedures for authorizing outsourcing of personal data processing defined?	Do the procedures for outsourcing of personal data processing correspond to the types of data filing systems that the company administers?	Do I known what the procedures are for outsourcing processing of personal data that I administer?
42	Are the scope and purpose of processing defined in the outsourcing contract?	Do the scope and purpose defined in the contract for outsourcing correspond to our scope and purpose of personal data processing?	
43	Does the contract include clauses about further outsourcing?	Are the clauses concerning further outsourcing in accordance with our scope of personal data processing and compliant with laws and regulations?	

No	Personal Data Controller or Managing Administrator	Administrator of Information Security (ABI)	Data Custodian (e.g. System/Application/Server)
44	Has the outsourcing contractor implemented required security measures?	How does the outsourcing contractor confirm having implemented the required security measures?	
45	Is the protection of outsourced personal data verified?	How is the the protection of outsourced personal data verified?	Do I take part in the verification of the protection of outsourced personal data?
46	Does the data transfer to outsourcing contractor fulfill security requirements?	How is the security of data transfer to outsourcing contractor ensured?	Do I transfer personal data in a secure way?
47	Does our company process outsourced personal data?	Which data filing systems are outsourced to our company for processing? Who authorized our company to process that data?	Does my system/application process personal data outsourced to my company?
48	Are the scope and purpose of data processing outsourced to our company defined?	What are the scope and purpose of data processing outsourced to our company?	Do I know what the scope and purpose of data processing outsourced to our company are?
49	Are procedures for processing data outsourced to our company defined?	What are the procedures for processing data outsourced to our company?	Do I know what the procedures for processing data outsourced to our company are?
50	Are there special security requirements concerning data outsourced to our company?	What are the special security requirements concerning data outsourced to our company? What data (parts) does it apply to?	Do I know the special security requirements concerning data outsourced to our company and processed in my systems?
Third countries (art. 31a, chapter 7)			
51	Is the personal data administrated by our company processed in a third country?	What personal data is processed in a third country?	Is personal data that I administer processed in a third country?
52		Who is the Polish representative of that party from a third country?	
53	Are data filling systems transferred to a third country?	What are the procedures concerning transfer of data filing systems to a third country?	Do I transfer data filing systems to a third country?
54		Is the third country in which processing personal data from us is taking place on the EU approved list?	
55	Are special requirements concerning transfer of data filing systems to a third country fulfilled?	What are the special requirements concerning transfer of data filing systems to a third country?	Are there special requirements for transfer of data filing systems (ranges of data) to a third country? Which data do they concern?
PROTECTION OF PERSONAL DATA			
Organisational safeguards (Art.31, Chapter 5) and the Regulation			
56	Are the regular information risk assessments performed?	What methodology of information risk analysis is used?	Do I take part in risk assessments concerning data filing systems that I administer?

No	Personal Data Controller or Managing Administrator	Administrator of Information Security (ABI)	Data Custodian (e.g. System/Application/Server)
57	Have the threats to personal data protection been identified? What are these threats?	What are the threats to specific categories of personal data?	What are the threats to my systems? What are these threats?
58	Are proper levels of data security defined for personal data processed in the company's systems?	Is the proper security level defined for each data filing system?	What level of data security is required for each data filing system that I administer?
59	Does the required documentation exist?	What documentation exists that describes ways of processing data and technical and organizational measures to protect personal data?	What documentation exists that describes ways of processing data and technical and organizational measures to protect personal data in the systems that I administer?
60	Do employees with authorized access for personal data sign the "data protection declaration"?	Where are the "data protection declarations" stored? Are they verified?	
61	What is the assurance that only authorized personnel can process personal data?	What is the procedure for authorizing personnel to process personal data? Do users processing personal data receive signed authorizations? Are copies of the authorisations archived?	Which users are authorized to access and process personal data in my systems? Am I authorized?
62	Is there a register of authorized users? What is the format of the register of authorized users?	Does the register of authorized users include their full names, dates of access granting and expiration, user ID in IS and scope of authorization?	Do I have the possibility to verify access authorizations to my systems?
63	Are the measures for accountability of data processing implemented?	What controls are implemented to make employees uniquely identifiable and accountable for access to data filing systems?	Are measures for accountability of data processing implemented in my systems?
64	Are the authorized users obliged to professional secrecy concerning personal data and its protection?	How are non-disclosure agreements stored?	
Documentation and training (art.39a and the Regulation)			
65	Is there a formal Information Security Policy (like ISO 27001) in the organisation?	Do I take part in developing and updating the Information Security Policy?	Do I know the Information Security Policy?
66	Are policies for personal data protection included in the Information Security Policy?	Which parts of the Information Security Policy concern personal data protection?	Do procedures and instructions in the Information Security Policy address personal data protection?
67	Has a security policy for personal data protection been developed and approved?	Does the security policy include requirements listed in the Regulation? (according to §4)	Do I take part in the development of the security policy?
68	Is the security policy for personal data protection up-to-date?	When and how was the security policy last verified?	Do I take part in the verification and update of the security policy?

No	Personal Data Controller or Managing Administrator	Administrator of Information Security (ABI)	Data Custodian (e.g. System/Application/Server)
69	Is the documentation describing data processing and security measures compliant?	What is the assurance that the documentation is up-to-date? Is it approved? Does it have a validity/verification date?	Do I have access to the current documentation?
70	Has an "Instruction for managing information systems" been developed and approved?	Does the "Instruction" include all elements required by the regulation? (according to §5)	Do I take part in the development of the "Instruction"?
71	Is the Instruction up-to-date?	When and how was the Instruction last verified?	Do I take part in the verification and update of the Instruction?
72	Has the documentation been implemented?	How were the security policy and Instruction implemented?	Do I know the security policy and Instruction?
73	Has the documentation been communicated to authorized users?	How do authorized users confirm that the documentation was communicated to them?	Have I read the documentation?
74		Is there additional documentation describing data processing and security measures?	Have I read the additional documentation?
75	Is training on data protection available to employees?	Am I responsible for the training?	Did I take part in training regarding personal data protection in our company?
Technical safeguards – confidentiality (art. 39a and the Regulation)			
76	Are there the zones of personal data processing?	Are there the zones of personal data processing?	Do I know the zones of personal data processing?
77		Is access to zones of personal data processing secured and controlled?	Are my systems/application in secured and controlled zones?
78		What are the physical security measures used for IT equipment, databases and media containing personal data?	What are the physical security measures used to protect my systems?
79		Who is responsible for the physical security of IT equipment, databases and media containing personal data?	Who is responsible for the physical security of my systems?
80		Are unauthorized persons visiting zones of personal data processing only under supervision by authorized staff?	Are unauthorized persons visiting "my" personal data processing zone only under supervision?
81		Do IT systems have access control with authentication and authorization features?	Do systems that I administer have access control with authentication and authorization features?
82		How are access rights granted to the systems verified?	Are access rights to my systems verified?
83		Do user access rules include setting password length, syntax and expiration date in accordance with the defined security level?	What user access rules are used in my systems?

No	Personal Data Controller or Managing Administrator	Administrator of Information Security (ABI)	Data Custodian (e.g. System/Application/Server)
84		Are the media containing personal data properly erased before their reuse, repair or handing over to an unauthorized person?	Are the media containing personal data from my systems properly erased before their reuse, repair or handing over to an unauthorized person?
85		Do we need to use cryptographic methods for transfer of personal data?	What cryptographic methods are used to transfer data from/to my systems?
86		Are physical and logical security measures used to protect access from/to a public network?	What physical and logical security measures are used to protect access from/to my systems to/from a public network?
87		Is additional protection implemented on portable devices (e.g. laptops) which contain personal data?	Are the data from my filling systems processed on portable devices? What kind of special protection is implemented?
88		What additional security measures are used to protect the confidentiality of personal data?	What additional security measures are used to protect the confidentiality of personal data in my systems?
Technical safeguards – integrity (art. 39a and the Regulation)			
89		Do systems log information about time of data entry and user ID?	Do my systems log information about time of data entry and user ID?
90		Is information about access and changes automatically logged?	Is information about access and changes in my systems automatically logged?
91		Do systems log information about the data source, if it is not from the data subject?	Do my systems log information about the data source, if it is not from the data subject?
92		Are physical and logical security measures used to protect access from/to a public network?	What physical and logical security measures are used to protect access from/to my systems to/from a public network?
93		What additional security measures are used to protect the integrity of personal data?	What additional security measures are used to protect the integrity of personal data in my systems?
Technical safeguards – availability (art. 39a and the Regulation)			
94		What are the security systems (alarms, fire/smoke detection, suppression systems) and environment control systems (temperature, humidity) installed in the rooms where information systems, databases or media with personal data are located?	What security and environment control systems are installed in the rooms where my systems are located?
95		Who is responsible for the security and environment control systems?	Who is responsible for the security and environment control of my systems?
96		Are backups made and are they protected in the same way as the master data?	Are backups of my systems made? Where are they stored?

No	Personal Data Controller or Managing Administrator	Administrator of Information Security (ABI)	Data Custodian (e.g. System/Application/Server)
97		How do we ensure that access to backups is limited and strictly controlled?	How do we limit and control access to backups?
98	Who is responsible for setting data retention dates?	Who sets the retention dates and who verifies the fulfillment of this requirement? How?	What are the retention dates set for data entrusted to me and how I fulfill them?
99		Are UPS systems installed to ensure processing continuity?	Are my systems protected against power outages and fluctuations?
100		Is securing availability of the data a part of the BCP/DRP plan?	
101		What additional security measures are used to protect the availability of personal data?	What additional security measures are used to protect the availability of personal data in my systems?
Monitoring of security (art. 39a and the Regulation)			
102	Are the implemented security measures monitored?	How are the implemented security measures monitored?	Are the security measures implemented in my systems monitored? How are they monitored?
103		How are the results of the monitoring of implemented security registered?	Did negative results of the monitoring concern my systems?
104		How were the recommendations resulting from the monitoring implemented?	Do any recommendations concern my systems?
Internal Control			
105	Is the internal audit division involved in verifying protection of personal data processing?	When was the last internal audit?	Did internal audits refer to my systems?
106		What are the conclusions and recommendations from the internal audit?	Did the recommendations concern my systems?
107		Is there a plan for implementing these recommendations?	Is there a plan for implementing recommendations concerning my systems?
108	Were all recommendations implemented?	Were the recommendations implemented?	Have I implemented the recommendations?
Rendering anonymous (art. 2)			
109	Are the data filing systems, which should no longer be processed, deleted or rendered anonymous?	How are the data filing systems, which should no longer be processed, deleted or rendered anonymous? What are the procedures? How is it documented?	How are the data filing systems, which should no longer be processed, deleted or rendered anonymous in my systems? How is it documented?
EXTERNAL COMMUNICATION			
GIODO (Chapter 2)			
110	Are the procedures for cooperation with GIODO during an inspection defined?	What are the procedures for cooperation with GIODO during an inspection?	Am I to take part in a GIODO inspection?

No	Personal Data Controller or Managing Administrator	Administrator of Information Security (ABI)	Data Custodian (e.g. System/Application/Server)
111	Are the procedures for registering data filing systems at GIODO defined?	What are the procedures for registering data filing systems at GIODO?	Are data filing systems processed in my systems registered at GIODO?
112		Do we use E-GIODO to register data filing systems?	
Data Subject (Chapter 4)			
113	Are data subjects informed that their data is collected?	How does the data controller inform about data collection?	
114	Are the procedures regarding the fulfillment of rights of the data subject defined?	What are the procedures regarding the fulfillment of rights of the data subject (Chapter 4)?	Can my system/application provide a printout of personal data in a readable form at the request of a data subject?
115	Are the procedures to stop processing of personal data if a data subject objects to it defined?	What are the procedures to stop processing of personal data if a data subject objects to it?	
Other regulations (art. 4, 5)			
116	Do other laws and/or international regulations apply to personal data processing in our company?	What other laws and/or international regulations apply to personal data processing in our company?	Do other laws and/or international regulations apply to personal data processed in my systems?
External audits			
117	Did external audits concern personal data processing?	When was the last external audit performed?	Did the external audit concern my systems?
118		What were the conclusions and recommendations?	Did the recommendations concern my systems?
119		Were these recommendations implemented?	Have I implemented these recommendations?

2.3. Mapping

2.3.1 COBIT Framework

COBIT® (Control Objectives for Information and Related Technology) is an IT governance framework, that allows managers to develop good practices for IT control in their enterprise and to organise IT activities within defined IT processes and domains. The latest version COBIT 4.1 emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework.

Using the COBIT framework to manage and control information systems can help in assessing and attaining compliance with UODO.

COBIT 4.1 Framework identifies:

- 4 IT domains :
  PO - Plan and Organise
  AI - Acquire and Implement
  DS - Deliver and Support
  ME - Monitor and Evaluate
- 34 IT processes,
- 210 IT control objectives organised by IT processes,
- 7 information criteria: effectiveness, efficiency, confidentiality, integrity, availability, compliance, reliability,
- 4 IT resources: applications, information, infrastructure, people,
- application controls (AC), defined as controls embedded within automated solutions,
- RACI charts, with guidance on roles and responsibilities for activities defined for each IT process; illustrate who is accountable (A), responsible (R), consulted (C) or informed (I),
- metrics defined for each IT process- measure how these processes support business and IT objectives; include: key performance indicators (KPI), key process goal indicators and key IT goal indicators (KGI),
- process maturity levels: non-existant (0), initial / ad-hoc (1), repeatable (2), defined (3), managed (4) or optimised (5).

To make use of the COBIT framework in ensuring compliance of information systems with UODO, the following manuals published by the IT Governance Institute® can be referred to:

- COBIT 4.1 [1], includes Management Guidelines,
- COBIT® Control Practices [2], includes control practices for each control objective,
- IT Assurance Guide using COBIT® [3], includes a variety of assurance activities.

The tables below include a mapping of UODO and Regulation articles to control objectives of the COBIT 4.1 framework. A mapping to control objectives defined in COBIT 3rd Edition [4] is also included.

2.3.2 UODO/COBIT

UODO	COBIT 4.0	COBIT 3rd Edition
CHAPTER 1 General Provisions		
Article 1	ME3.1-4	PO8.1, PO8.2
Article 2	ME3.1-4, PO2.2	PO8.1, PO8.2, PO2.2
Article 3	ME3.1-4	PO8.1, PO8.2
Article 3a	ME3.1-4	PO8.1, PO8.2
Article 4	ME3.1-4	PO8.1, PO8.2
Article 5	ME3.1-4	PO8.1, PO8.2
Article 6	ME3.1-4	PO8.1, PO8.2, PO2.2
Article 7	ME3.1-4, PO2.2	PO8.1, PO8.2
CHAPTER 2 Supervisory Authority for Personal Data Protection		
Article 8, 9, 10, 11, 12, 12a, 13 – not applicable		
Article 14	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Article 15	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Article 16	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Article 17	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Article 18	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Article 19, 20, 21, 22, 22a – not applicable		
CHAPTER 3 The Principles of Personal Data Processing		
Article 23	ME3.1-4, PO4.9, PO6.3	PO8.1, PO8.2, PO4.7, PO4.8, PO6.2
Article 24	ME3.1-4, PO4.8-9, PO4.15, PO6.3	PO8.1, PO8.2, PO4.6, PO4.7, PO4.15, PO6.2
Article 25	ME3.1-4, PO4.8-9, PO4.15, PO6.3	PO8.1, PO8.2, PO4.6, PO4.7, PO4.15, PO6.2
Article 26	ME3.1-4, PO2.3, PO4.8-9, PO6.3, DS11.2, DS11.4	PO8.1, PO8.2, PO2.2, PO4.7, PO4.8, PO6.2, DS11.19-22
Article 26a	ME3.1-4, PO6.3, AI2.3, AC5	PO8.1, PO8.2, PO6.2, DS11.12
Article 27	ME3.1-4, PO2.3, PO6.3, AC1	PO8.1, PO8.2, PO2.2, PO6.2, DS11.1
Article 28	ME3.1-4, PO2.3, PO6.3	PO8.1, PO8.2, PO2.2, PO6.2
Article 29	ME3.1-4, PO2.3, PO6.3, AC5, AC6	PO8.1, PO8.2, PO6.2, DS2.7, DS5.8, DS11.12-13, DS11.16
Article 30	ME3.1-4, PO6.3, AC5, AC6	PO8.1, PO8.2, PO6.2, DS11.12-13, DS11.16
Article 31	ME3.1-4, PO2.3, PO4.15, PO6.3, AI5.2, DS2.3-4, DS5.11, AC5, AC6	PO8.1, PO8.2, PO4.15, PO6.2, DS2.3, DS2.5, DS2.7-8, DS5.8, DS11.17
Article 31a	ME3.1-4, PO6.3	PO8.1, PO8.2, PO8.4, PO6.2
CHAPTER 4 The Rights of the Data Subject		
Article 32	ME3.1-4, PO4.15, DS8.1-4	PO8.1, PO8.2, PO4.15, DS10.1
Article 33	ME3.1-4, PO4.15, DS8.1-4	PO8.1, PO8.2, PO4.15, DS10.1

UODO	COBIT 4.0	COBIT 3rd Edition
Article 34	ME3.1-4, PO4.15, DS8.1-4	PO8.1, PO8.2, PO4.15, DS10.1
Article 35	ME3.1-4, PO4.15, PO6.3, DS8.1-4	PO8.1, PO8.2, PO4.15, PO6.2, DS10.1
CHAPTER 5 Protection of Personal Data		
Article 36	ME3.1-4, PO2.3, PO4.6, PO4.8, PO4.15, PO6.1-3, DS5.1-2, DS5.5	PO8.1, PO8.2, PO4.4, PO4.6, PO6.8, PO6.11, DS5.1-11, DS7.3
Article 37	ME3.1-4, PO4.8-9, DS5.4	PO8.1, PO8.2, PO4.7, PO4.8
Article 38	ME3.1-4, DS11.6, AC1, AC2, AC5	PO8.1, PO8.2, DS11.6, DS11.12, DS11.13, DS11.16
Article 39	ME3.1-4, PO4.15, DS5.3-4	PO8.1, PO8.2, PO4.15, PO6.8, PO6.11, DS5.4, DS7.3
Article 39a – separate list		
CHAPTER 6 Registration of Personal Data Filing Systems		
Article 40	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Article 41	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Article 42	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Article 43	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Article 44	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Article 44a	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Article 45 - (deleted)		
Article 46	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Article 46a	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
CHAPTER 7 Transfer of Personal Data to a Third Country		
Article 47	ME3.1-4, AC6	PO8.1, PO8.2, PO8.4, DS11.17
Article 48	ME3.1-4, AC6	PO8.1, PO8.2, PO8.4, DS11.17

2.3.3 Regulation/COBIT

Regulation	COBIT 4.1	COBIT 3rd Edition
§ 1.	ME3.1-4, PO6.2	PO8.1, PO8.2, PO6.8
§ 2.	ME3.1-4	PO8.1, PO8.2
§ 3.	PO4.8, DS5.2	PO4.6, DS5.1
§ 4.	PO2.2-3, DS5.2, DS5.7, DS5.10, DS12.1-2	PO2.2, PO6.8, DS5.1, DS12.1
§ 5.	PO6.2	PO6.8
pt 1)	DS5.3-4	DS5.2-6, DS5.9
pt 2)	AI2.3-4, DS5.3-4	DS5.2-6, DS5.9
pt 3)	PO7.8	DS5.2-6, DS5.9
pt 4)	DS11.5	DS11.19-22, DS11.26
pt 5)	DS11.2-5	DS11.19-22, DS11.26
pt 6)	DS5.9	DS5.19
pt 7)	PO2.3, AC5	DS2.7, DS5.8, DS11.16
pt 8)	AI1.1, AI2.10, DS5.2	DS5.1
§ 6.	PO2.3, DS5.1-4, DS5.7-8, DS5.10-11	PO2.2, PO2.4, DS5.8
security level A	DS5.3-4, DS5.8-9, DS11.2-6, DS12.3, DS12.5	
security level B	same as level A + DS5.11	
security level C	same as level A + DS5.10-11	
§ 7.	PO2.2, DS5.3	PO2.2, DS5.2, DS5.4
§ 8.	ME3.1-4	PO8.1, PO8.2
§ 9.	ME3.1-4	PO8.1, PO8.2
§ 10.	ME3.1-4	PO8.1, PO8.2

2.4. Using COBIT 4.1 to verify compliance with UODO

By knowing which IT control objectives[1] apply to information systems processing personal data we can use the COBIT framework to determine relevant controls[2] and control practices[3] to ensure compliance with UODO. COBIT can also help determine the metrics and maturity levels of IT processes applicable to verify compliance with UODO.

2.4.1 Example

The table below includes guidance on how to use the COBIT framework with art.26 of UODO and control objective DS11.2 as an example.

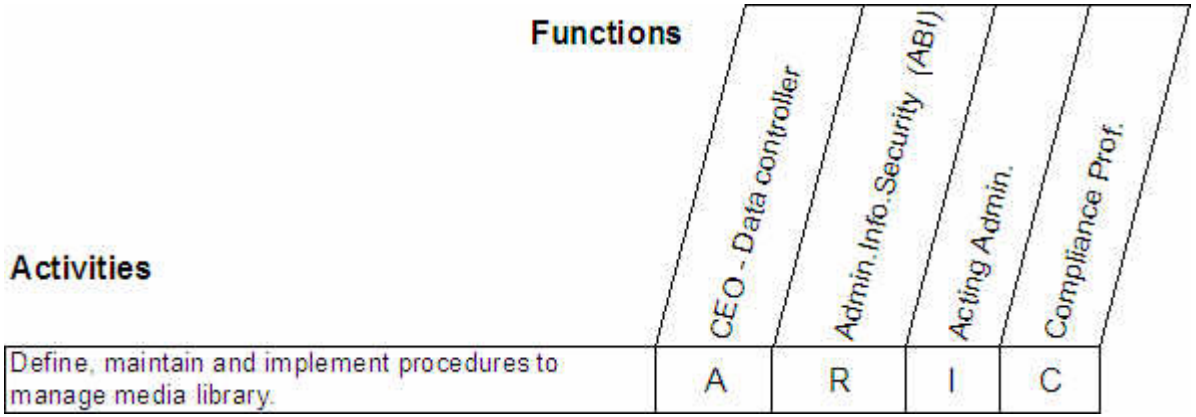
MAPPING		
UODO	**COBIT 4.0**	**COBIT 3rd Edition**
Article 26 states: 1. The controller performing the processing of data should protect the interests of data subjects with due care, and in particular to ensure that: 1)… 3)… 4) the data are kept in a form which permits identification of the data subjects no longer than it is necessary for the purposes for which they are processed. 2.	ME3.1-4, PO2.3, PO4.8-9, PO6.3, **DS11.2** DS11.4	PO8.1, PO8.2, PO2.2, PO4.7, PO4.8, PO6.2, DS11.19-22

[1] Control objective - A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process. Control objectives defined in the COBIT framework provide a complete set of high-level requirements to be considered by management for effective control of each IT process. Each IT process has a number of control objectives.

[2] Control - defined as the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

[3] Control practices - provide the how, why and what to implement for each control objective to improve IT performance and/or address IT solution and service delivery risks.

<table>
<tr><th colspan="3">COBIT Control objective: DS11.2 Storage and Retention Arrangements</th></tr>
<tr><td colspan="3">Define and implement procedures for effective and efficient data storage, retention and archiving to meet business objectives, the organisation’s security policy and regulatory requirements.</td></tr>
<tr><th>COBIT 4.1 publication</th><th>Usage</th><th>Example</th></tr>
<tr><td rowspan="4">COBIT 4.1

Framework
Control
Objectives
Management
Guidelines
Maturity Models</td><td rowspan="4">Can be used to:
- link business goals to IT goals,
- measure their achievement using provided metrics and maturity models,
- identify the associated responsibilities of business and IT process owners,
- define the management control objectives to be considered,
- identify the major IT resources to be leveraged</td><td>Key activity:
Define, maintain and implement procedures to manage the media library</td></tr>
<tr><td>Key activity goal:
Managing onsite and offsite storage of data</td></tr>
<tr><td>Key metrics:
- Number of incidents where sensitive data were retrieved after media were disposed of
- Number of incidents of noncompliance with laws due to storage management issues</td></tr>
<tr><td>RACI chart:
 
</td></tr>
<tr><td>COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition</td><td>Can be used to provide the how, why and what to implement for the control objective to improve IT performance and/or address IT solution and service delivery risks.
Support the prevention, detection and correction of undesired events through responsible use of</td><td>Control practice:
2. Establish storage and retention arrangements to satisfy legal, regulatory and business requirements for documents, data, archives, programmes, reports and messages (incoming and outgoing)</td></tr>
</table>

	resources, appropriate management of risk and the delivery of value to business.	
	Include value and risk statements to help articulate why it is worthwhile to implement the control objective	**Risk driver**: *Non-compliance with regulatory and legal obligations*
The IT Assurance Guide: Using COBIT®	Can be used to provide reliable assurance on internal controls, process improvement, financial support audit, etc. and support opinions and recommendations regarding proposed improvements	**Test the control design of the control objective**: *Review retention periods for data, and ensure that they are in line with contractual, legal and regulatory requirements*
		Test the outcome of the control objective: *Inspect the data management tools to make sure that they are being used as described*
		Document the impact of the control weaknesses: *Verify that consideration is given to the confidentiality, integrity and availability of the data as well as applicable laws and regulations*

3. APPENDIX

3.1. References

3.1.1 Published by IT Governance Institute®

Available at www.itgi.org and www.isaca.org.
Access to documents marked 🔓 is granted after free registration on the ISACA website.
Access to documents marked 🔒 is limited to ISACA members.

[1] COBIT 4.1 🔓
[2] COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition (dostępne tylko w księgarni ISACA)
[3] IT Assurance Guide using COBIT® 🔒
[4] COBIT® 3rd Edition Control Objectives (wycofane)
[5] COBIT Security Baseline™: An Information Security Survival Kit, 2nd Edition 🔒
[6] COBIT Mapping Overview of International IT Guidance, 2nd Edition
[7] COBIT Mapping: Mapping of ISO/IEC 17799: 2005 With COBIT 4.0 🔒
[8] Aligning COBIT®, ITIL® and ISO 17799 for Business Benefit

3.1.2 Published by ISACA®

[9] G31 IS Auditing Guideline: Privacy

3.1.3 Published by GIODO

Developed by the IT Department of the Bureau of the Inspector General for the Protection of Personal Data (available at www.giodo.gov.pl)

[10] Guidelines for the design and implementation of a security policy,
[11] Recommendations on developing an instruction for managing information systems processing personal data, including specific requirements for information security,
[12] Requirements for the structures of personal data filing systems and the functionality of the applications used for their management.

3.1.4 Published by APDCM

[13] e-PRODAT: e-Government and Data Protection in European Regions and Cities

3.1.5 Published by Kantor Wydawniczy ZAKAMYCZE

[14] Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz – “Ochrona danych osobowych – komentarz”, wyd.3, 2004, Kantor Wydawniczy ZAKAMYCZE

3.2. Dictionary

This dictionary includes terms associated with the protection of personal data in information systems. It was compiled to help using documents written in English.

Explanation:

- col.1 – term associated with the protection of personal data,
- col.2 – definition of term used in UODO or Regulation,
- col.3 – UODO article or paragraph of Regulation that includes the definition of the term,
- col.4 – corresponding English term used in the official English translation of UODO,
- col.5 – corresponding term used in COBIT,
- col.6 – corresponding term used in the IS Audit Guideline Privacy,
- col.7 – corresponding term used in laws of other countries.

Term in Polish	Definition of term used in UODO	Art.	Term in English	COBIT	IS Audit Guideline - Privacy	Laws of other countries [x]
1	2	3	4	5	6	7
administrator bezpieczeństwa informacji ABI	nadzorujący przestrzegania zasad ochrony	art. 36	administrator of information security	information security manager	privacy officer	internal data protection officer (HU)
administrator danych osobowych	organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania danych osobowych	art. 7 (art. 3)	controller	management	data controller	chief processor (EE)
administrator systemu, bazy danych, aplikacji		-		data custodian	data custodian	
anonimizacja danych		art. 2	data rendered anonymous			data rendered unidentifiable (AU)
dane doraźne	sporządzane wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji	art. 2	data files prepared ad hoc			
dane osobowe	wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej	art. 6	personal data		- personal data / information - personally identifiable information	
dane wrażliwe		-		sensitive information	sensitive data	sensitive data
firma trzecia	podmiot, któremu powierzono przetwarzanie danych	art. 31	another subject	third-party	external partner	processor (AU,CZ,GR) authorised processor (EE)
gromadzenie danych		-			data collection	collection of data (AU)
hasło	ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym	§ 2		password		

[x] Other countries: AU-Austria, CZ- Czech Republic, D- Germany, EE- Estonia, GR- Greece, HU- Hungary

Term in Polish	Definition of term used in UODO	Art.	Term in English	COBIT	IS Audit Guideline - Privacy	Laws of other countries *
1	2	3	4	5	6	7
identyfikator użytkownika	ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym	§ 2		user ID	user ID	
instrukcja	zawartość określona w par.5 Rozporządzenia	§ 5		security plan	security plan	
integralność	właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany	§ 2		integrity	integrity	
kategoria danych		art. 36		data classification		
kontrola dostępu	dotyczy dostępu do danych osobowych	zał.II		access control	access control	
kopia zapasowa	dotyczy zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania	§ 5		back-up	data back-up	
likwidacja	pozbawienie nośnika zapisu danych, a w przypadku gdy nie jest to możliwe, uszkodzenie go w sposób uniemożliwiający ich odczytanie;	zał.VI		disposal		
odbiorca danych	każdy, komu udostępnia się dane osobowe (z wyjątkami)	art. 7	data recipient	user	third party	third person (EE)
	oprogramowanie, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego	zał.III		malicious software	malicious software	
osoba, której dane dotyczą	osoba fizyczna, której dane osobowe są lub mogą być przetwarzane w zbiorach danych	art. 2	data subject		data subject	
państwo trzecie	państwo nie należące do Europejskiego Obszaru Gospodarczego	art. 7	third country			
polityka bezpieczeństwa	zawartość określona w par.4 Rozporządzenia	§ 4		security policy	security policy	
poufność	właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom	§ 2		confidentiality	confidentiality	

Term in Polish	Definition of term used in UODO	Art.	Term in English	COBIT	IS Audit Guideline - Privacy	Laws of other countries *
1	2	3	4	5	6	7
powierzenie przetwarzania danych		art. 31	authorise another subject to carry out the processing	outsourcing	outsourcing	committing of data (AU)
przekazanie danych	przekazanie danych osobowych innemu administratorowi danych	art. 38	transfer of data		transfer of data	
przekazanie danych za granicę	Przekazanie danych osobowych do państwa trzeciego	rozdz.7	transfer of data to a third country	transborder data flow	transborder flow of personal data	transfer abroad (D) transmission to foreign states (EE) transboundary flow (GR)
przetwarzanie danych	jakiekolwiek operacje wykonywane na danych osobowych	art. 7	processing of data	processing of data	treatment of personal information	
raport	przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych	§ 2		output		
rejestracja zbiorów danych	zgłoszenie zbioru danych do GIODO	rozdz. 6	registration of personal data filing systems			registration in the Data Processing Register (AU)
rozliczalność	właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi	§ 2	ability to map a given activity or event back to the responsible party	accountability	accountability	
sieć publiczna	sieć telekomunikacyjna nie będąca siecią wewnętrzną, służąca do świadczenia usług telekomunikacyjnych	§ 2		public network		

Term in Polish	Definition of term used in UODO	Art.	Term in English	COBIT	IS Audit Guideline - Privacy	Laws of other countries *
1	2	3	4	5	6	7
sieć telekomunikacyjna	urządzenia telekomunikacyjne i linie telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną	§ 2		telecommunications		
środki bezpieczeństwa	środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną	§ 6		security measures	security measures / safeguards	
teletransmisja	przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej	§ 2		transmission		
udostępnienie danych	udostępnienie posiadanych w zbiorze danych innym osobom lub podmiotom	art.29,30	disclosure of data	disclosure	disclosure	
uprawnienia	dotyczy przetwarzania danych	§ 5		user authorisation	access privileges	
usuwanie danych	zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą	art.7	data erasure	deletion	data erasure / deletion / destruction	personal data liquidation (CZ)
uwierzytelnianie	działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu	§ 2		user authentication		
właściciel danych		-		data owner	information owner	
zabezpieczenie danych	w systemie informatycznym	art. 7 rozdz. 5	- security of data - protection of personal data	data security	- personal information protection / security - privacy controls	
zbiór danych osobowych	każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów	art. 7	data filing system	database	personal database	data file (CZ) file (GR)

3.3. Mappings

3.3.1 UODO/COBIT 4.1 - PO, AI, ME domains

COBIT 4.1	ME3				PO2		PO4				PO6			AI2	AI5
UODO	3.1	3.2	3.3	3.4	2.2	2.3	4.6	4.8	4.9	4.15	6.1	6.2	6.3	2.3	5.2
1	X	X	X	X											
2	X	X	X	X	X										
3	X	X	X	X											
3a	X	X	X	X											
4	X	X	X	X											
5	X	X	X	X											
6	X	X	X	X											
7	X	X	X	X	X										
14	X	X	X	X									X		
15	X	X	X	X									X		
16	X	X	X	X									X		
17	X	X	X	X									X		
18	X	X	X	X									X		
23	X	X	X	X					X				X		
24	X	X	X	X				X	X	X			X		
25	X	X	X	X				X	X	X			X		
26	X	X	X	X		X		X	X				X		
26a	X	X	X	X									X	X	
27	X	X	X	X		X							X		
28	X	X	X	X		X							X		
29	X	X	X	X		X							X		
30	X	X	X	X									X		
31	X	X	X	X		X				X			X		X
31a	X	X	X	X									X		
32	X	X	X	X						X					
33	X	X	X	X						X					
34	X	X	X	X						X					
35	X	X	X	X						X			X		

COBIT 4.1	ME3				PO2		PO4				PO6			AI2	AI5
UODO	3.1	3.2	3.3	3.4	2.2	2.3	4.6	4.8	4.9	4.15	6.1	6.2	6.3	2.3	5.2
36	X	X	X	X		X	X	X		X	X	X	X		
37	X	X	X	X				X	X						
38	X	X	X	X											
39	X	X	X	X						X					
40	X	X	X	X									X		
41	X	X	X	X									X		
42	X	X	X	X									X		
43	X	X	X	X									X		
44	X	X	X	X									X		
44a	X	X	X	X									X		
46	X	X	X	X									X		
46a	X	X	X	X									X		
47	X	X	X	X											
48	X	X	X	X											

3.3.2 UODO/COBIT 4.1 - DS domain and ACs

COBIT 4.1	DS2		DS5						DS8				DS11			AC					
UODO	2.3	2.4	5.1	5.2	5.3	5.4	5.5	5.11	8.1	8.2	8.3	8.4	11.2	11.4	11.6	1	2	3	4	5	6
23																					
24																					
25																					
26													X	X							
26a																				X	
27																X					
28																					
29																				X	X
30																				X	X
31	X	X						X												X	X
31a																					
32									X	X	X	X									
33									X	X	X	X									
34									X	X	X	X									
35									X	X	X	X									
36			X	X			X														
37						X															
38															X	X	X			X	
39					X	X															
47																					X
48																					X

3.3.3 Regulation/COBIT 4.1

COBIT 4.1	ME3				PO2		PO4	PO6	PO7	AI1	AI2			AC
Regul.	3.1	3.2	3.3	3.4	2.2	2.3	4.8	6.2	7.8	1.1	2.3	2.4	2.10	16
§ 1	X	X	X	X				X						
§ 2	X	X	X	X										
§ 3							X							
§ 4					X	X								
§ 5								X						
Item 1														
2											X	X		
3									X					
4														
5														
6														
7						X								X
8										X			X	
§ 6						X								
§ 7					X									
§ 8	X	X	X	X										
§ 9	X	X	X	X										
§ 10	X	X	X	X										

Regulation/COBIT 4.1 – cont.

COBIT 4.0	DS5									DS11					DS12			
Regul.	5.1	5.2	5.3	5.4	5.7	5.8	5.9	5.10	5.11	11.2	11.3	11.4	11.5	11.6	12.1	12.2	12.3	12.5
§ 1																		
§ 2																		
§ 3		X																
§ 4		X			X			X							X	X		
§ 5																		
Item 1			X	X														
2			X	X														
3																		
4													X					
5										X	X	X	X					
6							X											
7																		
8		X																
§ 6	X	X	X	X	X	X		X	X									
A			X	X		X	X			X	X	X	X	X			X	X
B			X	X		X	X		X	X	X	X	X	X			X	X
C			X	X		X	X	X	X	X	X	X	X	X			X	X
§ 7			X															
§ 8																		
§ 9																		
§ 10																		