



Title: *D7.1a User Evaluation Plan*

Author: *Johann Schrammel (Center for Usability Research & Engineering)*
Eva Ganglbauer (Center for Usability Research & Engineering)
Eleni Kosta (Katholieke Universiteit Leuven - Interdisciplinary Centre for Law and ICT)

Editor: *Eva Ganglbauer (Center for Usability Research & Engineering)*

Reviewers: *Stefan Eicker (IT-Objects GmbH)*
José Luis Vivas (Universidad de Málaga)

Identifier: *D7.1a*

Type: *Deliverable*

Version: *1.0*

Date: *15/12/2009*

Status: *Final*

Class: *Public*

Summary

In this deliverable we describe a comprehensive trial and assessment plan for the first evaluation phase. The plan includes information regarding testing scenarios, methods, metrics, selection of users, and timing. Additionally this deliverable includes a summary of the set up of the PICOS Angling Community Prototype field trials & lab test and legal analysis of the collection and processing of personal data. As PICOS' mission is to protect privacy and enable trust and security, the legal analysis also includes a privacy policy for the project, a user consent form that was signed by the users for the trials in Vienna and in Kiel and a country report. The country report contains legal information important for PICOS about the United Kingdom and Germany, as their legal systems are quite different: the United Kingdom has a common law legal system and Germany a continental law one. As PICOS is going to be deployed in various European Member States, we wanted to make an analysis of two countries with different legal system in order to ensure the potential deployment of PICOS throughout Europe. In general the data protection legal frameworks of the European Member States are based on EU Directives and therefore no major differences are found among them. Our country analysis addresses in turn the most pertinent aspects of data protection law in the context of electronic communications networks and services, with a focus on mobile communications, as well as some other relevant law. The goal of the analysis is to assure that the innovative concepts of Picos are conforming to the law in the European Member States



Grant Agreement no. 215056

Members of the PICOS consortium:

Johann Wolfgang Goethe-Universität (Coordinator)	Germany
Hewlett-Packard Laboratories Bristol	United Kingdom
Hewlett-Packard Centre de Competence France	France
Universidad de Málaga	Spain
Center for Usability Research & Engineering	Austria
Katholieke Universiteit Leuven	Belgium
IT-Objects GmbH.	Germany
Atos Origin	Spain
T-Mobile International AG	Germany
Leibniz Institute of Marine Sciences	Germany
Masaryk University	Czech Republic

The PICOS Deliverable Series

D2.1 Taxonomy	July 2008
D2.2 Categorisation of Communities	July 2008
D2.3 Contextual Framework	November 2008
D2.4 Requirements	November 2008
D4.1 Platform Architecture and Design v1	March 2009
D5.1 Platform description document v1	October 2009
D9.1 Web Presence	February 2008
D9.2.1 Exploitation Planning	April 2009
D9.3.1 Dissemination Planning	April 2009

These documents are all available on the project website located at <http://PICOS-project.eu>.



The PICOS Deliverable Series

Vision and Objectives of PICOS

With the emergence of services for professional and private online collaboration via the Internet, many European citizens spend work and leisure time in online communities. Users consciously leave private information; they may also leave personalized traces they are unaware of. The objective of the project is to advance the state of the art in technologies that provide privacy-enhanced identity and trust management features within complex community-supporting services that are built on Next Generation Networks and delivered by multiple communication service providers. The approach taken by the project is to research, develop, build trial and evaluate an open, privacy-respecting, trust-enabling platform that supports the provision of community services by mobile communication service providers.

The following PICOS materials are available from the project website <http://www.picos-project.eu>.

Planned PICOS documentation

- Slide presentations, press releases, and further public documents that outline the project objectives, approach, and expected results;
- PICOS global work plan provides an excerpt of the contract with the European Commission.

PICOS results

- *PICOS Foundation* for the technical work in PICOS is built by the categorization of communities, a common taxonomy, requirements, and a contextual framework for the PICOS platform research and development;
- *PICOS Platform Architecture and Design* provides the basis of the PICOS identity management platform;
- *PICOS Platform Prototype* demonstrates the provision of state-of-the-art privacy and trust technology to leisure and business communities;
- *Community Application Prototype* is built and used to validate the concepts of the platform architecture and design and their acceptability by covering scenarios of private and professional communities;
- *PICOS Trials* validate the acceptability of the PICOS concepts and approach chosen from the end-user point of view;
- *PICOS Evaluations* assess the prototypes from a technical, legal and social-economic perspective and result in conclusions and policy recommendations;
- *PICOS-related scientific publications* produced within the scope of the project.



Table of Contents

<i>List of acronyms</i>	6
1 User Evaluation Plan	8
1.1 Overview of evaluation activities in phase 1	8
1.2 Trial participants	9
1.3 Introduction and briefing to evaluation activities	9
1.4 Lab tests	10
1.4.1 Explanation of PICOS project context and concepts	10
1.4.2 Free exploration of the system	11
1.4.3 Qualitative Interview	11
1.4.4 Lab tasks (using mobile device)	11
1.4.5 Qualitative Interview	12
1.5 Field tests	12
1.5.1 Outdoor tasks	12
1.5.2 Questionnaires and Focus group	13
1.6 Field trials	13
1.6.1 Briefing in group setting	13
1.6.2 Actions initiated by virtual PICOS-friends	13
1.6.3 Angling competition	14
1.6.4 Further activities to enhance usage of PICOS system	15
1.6.5 DeBriefing and focus group	15
1.7 Resources	15
1.8 Timing	16
2 Country Report	18
2.1 United Kingdom	18
2.1.1 Introduction	18
2.1.2 Regulatory bodies and their powers	21
2.1.3 Personal Data	23
2.1.4 Processing of Personal Data	27
2.1.5 Traffic Data and its processing	38
2.1.6 Location Data and its processing	39
2.1.7 Rights of the Data Subject	41
2.1.8 Confidentiality of Communications	42
2.1.9 Direct Marketing	46
2.1.10 Data Retention	47
2.1.11 Other Relevant Laws	48



D7.1a User Evaluation Plan

2.1.12 Conclusion.....	50
2.2 Germany.....	51
2.2.1 Introduction.....	51
2.2.2 Regulatory bodies and their powers.....	53
2.2.3 Personal Data.....	58
2.2.4 Processing of Personal Data.....	59
2.2.5 Traffic Data and its processing.....	73
2.2.6 Location Data and its processing.....	74
2.2.7 Rights of the Data Subject.....	75
2.2.8 Confidentiality of Communications.....	78
2.2.9 Direct Marketing.....	79
2.2.10 Data Retention.....	80
2.2.11 Conclusion.....	82
2.3 Conclusion.....	82
2.4 Bibliography & References.....	82
3 Appendices.....	90
<i>Appendix I - User Consent form.....</i>	<i>90</i>
<i>Appendix II - Picos Privacy Policy.....</i>	<i>95</i>



List of acronyms

<i>AVMS</i>	<i>Audio-visual Media Services</i>
<i>BBC</i>	<i>British Broadcasting Corporation</i>
<i>BDSG</i>	<i>Bundesdatenschutzgesetz (Federal Data Protection Act)</i>
<i>BfDI</i>	<i>Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Federal Data Protection Commissioner)</i>
<i>BnetzA</i>	<i>Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen [short version Bundesnetzagentur (Regulatory Authority for Telecommunications and Posts)]</i>
<i>CPS</i>	<i>Crown Prosecution Service</i>
<i>DPA</i>	<i>Data Protection Act</i>
<i>DPD</i>	<i>Data Protection Directive</i>
<i>DPI</i>	<i>Deep Packet Inspection</i>
<i>DPO</i>	<i>Data Protection Official</i>
<i>DPP</i>	<i>Director of Public Prosecutions</i>
<i>DRR</i>	<i>Data Retention (EC Directive) Regulations 2009</i>
<i>EEA</i>	<i>European Economic Area</i>
<i>ECHR</i>	<i>European Convention on Human Rights</i>
<i>ECJ</i>	<i>European Court of Justice</i>
<i>ECNS</i>	<i>Electronic Communications Networks and Services</i>
<i>ECtHR</i>	<i>European Court of Human Rights</i>
<i>EU</i>	<i>European Union</i>
<i>GG</i>	<i>Grundgesetz für die Bundesrepublik Deutschland (Basic Law for the Federal Republic of Germany)</i>
<i>ICO</i>	<i>Information Commissioner's Office</i>
<i>IFG</i>	<i>Informationsfreiheitsgesetz (Freedom of Information Act)</i>
<i>IMSI</i>	<i>International Mobile Subscriber Identity</i>
<i>IMEI</i>	<i>International Mobile Equipment Identity</i>
<i>ISO</i>	<i>International Organisation for Standardisation</i>
<i>ISP</i>	<i>Internet Service Provider</i>



D7.1a User Evaluation Plan

<i>PECR</i>	<i>Privacy and Electronic Communications (EC Directive) Regulations</i>
<i>RIPA</i>	<i>Regulation of Investigatory Powers Act</i>
<i>RFID</i>	<i>Radio Frequency Identification</i>
<i>SCA</i>	<i>Serious Crime Act</i>
<i>TKG</i>	<i>Telekommunikationsgesetz (Telecommunications Act)</i>
<i>TMG</i>	<i>Telemediengesetz (German Telemedia Act)</i>
<i>TPS</i>	<i>Telephone Preference Service</i>
<i>TVWF</i>	<i>Television Without Frontiers</i>
<i>UID</i>	<i>Unique Identifier</i>
<i>UWG</i>	<i>Gesetz gegen den unlauteren Wettbewerb (Law against Unfair Competition)</i>
<i>UKAS</i>	<i>United Kingdom Accreditation Service</i>



1 User Evaluation Plan

This document describes the current state of planning for the PICOS field trials, based on the field trials outline plan (D2.5), the current version of the functional specification as provided by WP5 and the outcomes of several telephone conferences held until now with regard to this topic. This document also incorporates the comments and requests made by several partners in written form.

1.1 *Overview of evaluation activities in phase 1*

The general procedure of the evaluation activities in the first phase of PICOS will include several different interlinked steps; the main parts of this process are:

- Lab Test
- Field Tests
- Field trials

Evaluation activities will take place parallel in two tracks taking place at Vienna and Kiel. The lab tests and field tests are planned lasting a half day each, and take place in Vienna for the 27th and 28th of November 2009 and in Kiel for the 12th and 13th of December 2009. Selected users according to the trial needs will be invited to participate in the evaluation activities.

As a first activity these users will come to the Lab (CUREs usability lab in Vienna respectively a meeting room in Kiel provided by Bernd Ueberschär enhanced with CUREs mobile lab equipment such as recording and screen capturing equipment) and be introduced to the overall procedure and goals of the PICOS evaluation. Next they participate in the lab test, where the device is explained to them and they are asked to perform several tasks and are observed during the interaction (for a detailed specification see section 5).

The next day after the lab tests users are driven to nearby sites of the field test and asked to perform a specified set of tasks in this realistic environment (see section 6 for details). Field tests have a similar procedure to lab tests, but they take place in the actual application context i.e. in the 'field' and not in the lab. In the first evaluation phase of PICOS field tests will take place at two different sites. An angling spot near Vienna and an angling spot near Kiel will be selected for the field tests. After the field tests the participants are brought back and in a focus group setting in the lab in Vienna respectively Kiel the experiences during the field test are discussed.

Directly following this discussion the test participants are briefed regarding the field trials. In the field trials participants are encouraged to use the PICOS device and application freely for one month and to provide feedback on issues that arise. Trial participants take the device home with them and are free to interact with it as they want. However, to ensure activity several measures are taken by the PICOS team to encourage interaction and usage of the system. Since participants cannot be observed as in a lab test, they are asked to take notes, write diaries and fill in protocols; The field trial phase will last for one month and finish with another focus group event where participants are invited to come to a



closing focus group, where their experiences are discussed, the devices are collected and test participants can pick up their allowances.

The following sections provide details regarding the planning of the different parts of the first user evaluation.

1.2 Trial participants

Selected users will be invited to participate in the evaluation activities. In general we plan to conduct the evaluations with 3-4 groups a 4-6 persons (Vienna and Kiel). This means in total about 20 anglers will be involved in the evaluation activities. Trial participants are screened according to the following criteria:

- They must be active anglers
- Have interested in new technologies
- Are familiar with mobile devices
- Must be able to handle the application in English
- Are from diverse demographic backgrounds

Special effort will be taken to also find and invite people who already know each other within a group before the trials to allow and support for naturalistic interaction within the test communities.

1.3 Introduction and briefing to evaluation activities

The first step of the evaluation activities will be the introduction to the field test and briefing of participants. This will take place in the laboratory. We point out the goals of the evaluation activities and the different sessions and that the aim is to test the system but not the participant. The briefing phase is concluded by a short interview concerning some demographic data of the participants, such as age, education level, occupation, and level of experience. Furthermore the pre-questionnaire will contain items related to the following topics:

- Experience with mobile devices
- Experience with online communities
- Experience with specific angling community
- Expectations regarding a angling community
- Importance of privacy, trust, identities and security for the user

Next every participant will receive a Nokia 5800 with the installed application. As the participants can not be expected to use the mobile device without any explanation, they get a brief introduction to the usage. The basic technical functionality of the device is explained thoroughly to the participants. Every participant is given the same standardized explanation, which is followed by a short exploration



phase, where the participant may try his/her hand at the handling of the device. The participants then are asked to conduct the following training tasks to learn using the device:

- Turn on/off device
- Interacting by touch and with pen
- Navigate on screens /scrolling
- How to access different menus
- How to access the internet via Wi-Fi and via the GSM (with limited data transfer)
- Navigate to/between pages and applications
- Entering text and numbers in different contexts.
- Reset application in case of an abnormal system end.

In case participants have difficulties they can ask questions. Training tasks are repeated until participants are comfortable with all aspects of handling the device.

1.4 Lab tests

For the lab tests, users will be split into two groups, so for one lab tests 5 users will participate. E.g. 5 test participants attend Cure's lab for the tests before midday, the other 5 participants in the afternoon. The goal of a lab test is to evaluate the usability and user experience of the PICOS application with users of the real target groups. To be able to do so first, after the training of the device, the main concepts of the PICOS-project are explained to the users.

1.4.1 Explanation of PICOS project context and concepts

This explanation will contain the following elements:

- Service for angling community
- Allows to share information among anglers
- Stay in touch and share experiences
- Access to relevant data and information about angling
- Concepts of Community, public and private Sub-community, private room root identities and partial identities
- Handling mainly with mobile device
- There exists also a web access with restricted functions
- Special focus on privacy, trust, identity and security aspects

During this explanation both the mobile device and the web version of the system will be used to show and communicate the different concepts and possibilities of the PICOS system.



1.4.2 Free exploration of the system

Next test participants are asked to explore the system using both the mobile device and the web access. It is made clear by verbal statements of the test facilitators that the focus should be on the mobile device, but that also questions of how the two access possibilities work together are of interest. Free exploration time is limited to 10 minutes.

1.4.3 Qualitative Interview

Following the free exploration users are interviewed regarding the following topics:

- General impression of the application
- Problems, strengths and weaknesses
- If and how are privacy, trust and security supported by the application
- Further usage of the application
- Subjective satisfaction and user experience

1.4.4 Lab tasks (using mobile device)

After this introduction and exploration to the System and PICOS concepts test participants are asked to perform realistic tasks with the system. Here only the mobile device is used. Web access can be used to check the results of an interaction in case test participants wish to do so. The users' interaction with the system is observed and recorded for later analysis. After each task the test facilitator briefly asks the participants regarding encountered problems, difficulties and ideas for improvement. Additionally quantitative measures such as task completion rate and time, but also qualitative measures of subjective satisfaction and user experience will be collected for each task. The aim is to measure the current usability and user experience of the system, and to detect usability problems and their causes in order to improve the system's usability.

In detail the users will be asked to perform the following tasks in the lab using mobile device:

- Task of creating main public partial identity
- Search for contacts
- Invite other group members and PICOS-friends (Picos will create virtual identities (=PICOS-friends) before the test, who can be invited from test participants)
- Login, logout and exit of PICOS application
- Login again and change profile information, e.g. add age and email address
- Create a new partial identity
- Change to new partial identity
- Join a public sub-community and send message to all members of the sub-community
- Create a diary entry



- Change the diary entry from private to public
- Take a picture and upload it to the private room
- Add a comment to a friend's diary entry and rate it with the partial identity
- Create a more privacy sensitive partial identity
- Add a comment to a picture a friend has uploaded and rate it with your private partial identity
- Send a message to a contact
- Create a privacy policy
- Revocating and leaving from the community

1.4.5 Qualitative Interview

- General impression of the system
- Problems, strengths and weaknesses
- If and how are privacy, trust and security supported by the system
- Further usage of the system
- Subjective satisfaction and user experience
- Would users expect all data to be deleted after revocation

1.5 *Field tests*

The Outdoor field test takes place at a small fishing site with the whole group (10 persons). The users are positioned at different sites and are divided into three groups (3-4 persons per group). Two test facilitators are around to support and observe the tests. Every group will be given a sheet of paper with task descriptions.

1.5.1 Outdoor tasks

The test participants interact freely with the system. Afterwards, within a certain time frame (e.g. one hour) participants have to perform different tasks, which are:

- One participant has to create a private Sub-Community for the field tests
- Find friends who are around (close).
- Find fishing site “great carps” on the map and go there
- Add a comment on fish site description “great carp”
- Create a diary entry for the “great carps” spot when spatially there and blur position. Take a photo or record a video from this place and add it to the diary entry
- Find an fishing site close (similar to available functions in google maps)



1.5.2 Questionnaires and Focus group

Questionnaires to rate the PICOS applications on the mobile and on the web are filled in (SUS).

Finally there will be a focus group with all users after the outdoor tasks. It will include the discussion of experiences, privacy, trust, identity and security, and problems and possibilities for improvement.

After the focus group, participants and test facilitators will go to a restaurant and have dinner to encourage social interaction between participants. The community ties can be strengthened and informal communication can reveal further aspects of the application.

1.6 *Field trials*

1.6.1 Briefing in group setting

In user trials, participants use the system in their daily life. User trials are conducted spanning longer periods of time (e.g. some weeks). Users take devices home and are encouraged to interact with the system on their own. Since participants cannot be observed as in a lab test, they are asked to take notes, write diaries or fill in a protocol. Also - in contrast to lab and field tests - for trials the users are asked to use the system, and no specific tasks are defined. Additionally, interviews, questionnaires and focus groups can be used to gain more insights into the experiences the participants made while using the system.

Very active users will be granted with an extra remuneration (reputation and number of reasonable content created by the user). Two friends in the participant's buddy list will be controlled by us and interact with them (= virtual PICOS-friends). Participant's activities will be encouraged by interactions with these PICOS-friends to carry out certain actions. If a certain action such a friend request or an invitation to join a group is carried out, notifications are sent to the participants automatically, as common and helpful in communities. Special requests from virtual PICOS-friends will contain privacy- and security-critical tasks (e.g. the provision of private or security-sensitive data).

The field trials for the first cycle are planned for the months May and April. Due to weather conditions, April would be more preferable as the weather encourages more anglers to go outside in Vienna and Kiel and actually use the application in its real context.

Every participant will receive a compensation of 150€ for the field trials and be able to gain remunerations of 50€ if they actively use the PICOS application and create a lot of content and interact with each other. There is also the possibility for participants to keep the devices as compensation for the time they invested instead of taking the allowances.

1.6.2 Actions initiated by virtual PICOS-friends

There are two defined roles for virtual PICOS-friends:

1. One virtual PICOS-friend is known by the participants to be controlled by us. The name of the virtual PICOS-friend will be "**PICOS trial facilitator**".



2. The second virtual PICOS-friend is not known to be controlled by us. His name will be “**Florian Karner**” with low reputation. He will be controlled by us, but participants will believe him to be real as they don’t know this.
3. The third virtual PICOS-friend has a high reputation. His name will be “**Martin Ilic**” and he will also be controlled by us, although appearing to be a real person to the participants.

The virtual PICOS-friends will initiate several actions described below. We will only initiate actions that are supported by the functionalities of the first PICOS-prototype, so no further resources on it has to be carried out.

1. Participants should join a certain PICOS sub-community invited by “PICOS trial facilitator” and discuss topics (e.g. how they use the device, how often, what things do they like or dislike, experience reports and usage of applications with the device). If people are not participating in the discussions, they are several times invited by “PICOS trial facilitator”.
2. “Florian Karner”, an unknown member with low reputation invites participants to follow an external faked “funny angling application”. CURE will build this external fishing site. It will be possible to observe if people are agreeing to disclosing their email address and their data.
3. The “PICOS trial facilitator” sends a message to all participants. The first participant responding gains a 50€ voucher for the already existing online tackle shop.
4. A special remuneration is offered by “PICOS trial facilitator” for participants who go for an angling weekend, take the mobile device with them, use the PICOS application and create a catch diary entry.
5. An unknown PICOS-friend with high reputation (“Martin Ilic”) invites participants to join a sub-community he administers. The privacy advisor should act and we can observe, how participants will react.

1.6.3 Angling competition

Additionally, we plan a special outdoor angling competition event for anglers to provide the possibility for evaluating the mobile aspect of the PICOS application. A free exploration doesn’t guarantee if participants are using parts of the PICOS application we want to evaluate, although intervening in the natural interaction intended for a field trial.

The two meetings of PICOS field trial members will take place at an arranged angling spot near Vienna for Viennese anglers and near Kiel for anglers from Kiel. The competition event includes certain tasks for participants and aims at angling the biggest and/or the most fishes for one species. The field trial group is divided into two groups that are competing each other. Before the competition participants should carry out the following tasks:

1. Every group has to create a sub-community before the competition takes place to talk about the competition and the preparation for the event (which baits, etc.)
2. Participants should find out which other accessible angling catch diary entries exist for the place. Generally participants should inform themselves about the species that can be found in the lake.



3. An angling expert member in a special sub-community of that lake with a very high reputation can be requested.

The angling competition will aim at angling the biggest and/or the most fishes. Instant messaging between groups (one participant of one group chats with one participant of the competing group) helps to watch the progress of the other competing group. Moreover, instant messaging can be enhanced by uploading and demonstrating pictures and data of caught fishes.

Going from the competition outside to the inside, there will be a questionnaire first followed by a focus group and a short online debriefing interview.

1.6.4 Further activities to enhance usage of PICOS system

- All the information necessary for participants (e.g. the angling competition event) will be communicated by the “PICOS trial facilitator” via the PICOS system. Therefore we are encouraging participants using the PICOS system by communicating with it.
- Angling competition weekend to encourage further interaction of participants
- Extra remuneration for extra engagement of participants.

1.6.5 DeBriefing and focus group

Above the communication with the “PICOS trial facilitator” via the PICOS system, Cure and Ifm-Geomar will additionally provide direct communication and support for participants through a telephone helpline and emails.

Finally, one feedback focus group at CURE and one in Kiel is organized where the experiences in unrestricted use are discussed. The focus group will be carried out with an important aspect on privacy, trust, identities and security. The focus group will additionally broach the issues of

- General impression of the application
- Problems, strengths and weaknesses
- Demand for web front end
- Further usage of the application
- Subjective satisfaction and user experience

1.7 Resources

Resources of different type need to be available and all sorts of materials need to be prepared to ensure smooth running of the community trials. This section provides an outline of the most important things that have to be considered for the preparation of the trials.

The most important resource is a **working mature community prototype**. Due to its critical nature fall-back solutions in case of problems should be planned beforehand and stability of the system must be tested severely. The setup of the trials prototype must also include possibilities to log user interactions and provide access to these logs without disturbing the systems functioning.



For the mobile aspect of the community trials users will need Nokia 5800 devices to interact with the system, which will be provided by PICOS. The handsets will be obtained by HPF/L and UMA.

Costs coverage for the mobile connections to the PICOS System during the trials has to be organised. Different options exist, and detailed solutions have been identified to single out the most cost-effective solution for the trials. The costs for the user trials will be handled by Cure.

Meeting rooms at different sites will be required for the conduction of focus groups and interviews. Office space from projects partners will be used as far as possible, but also the need to organize some rooms on the market has to be expected.

An environment for experience sampling (triggering of samples, direction towards questionnaires, etc) and online diaries and questionnaires will be setup to allow efficient and ongoing analysis of data. Also a help desk for users with technical or methodological questions should be established for there duration of the trials.

The **helpline during the field phases needs to be organised**. It is planned to use a mobile phone, which is passed between the different partners Cure and Ifm-Geomar responsible for answering the help line. If the problems are of technical nature, the partners in charge will be informed and can take care of the problems during normal working days. In case that problems arise during the angling competition weekends, a technical support will be provided.

1.8 Timing

The community trials will take place in two phases in accordance with the overall projects planning. The following table summarizes the actions planned for PICOS and their timings on the basis of the angler community.

Phase 1	Scheduled
Trial plan	10-30-2009
Early prototype testing	Q3-Q4 2009
Lab testing (with selected members of the angling community)	Vienna: 11-27-2009 Kiel: 12-12-2009
Field tests (with a number of selected anglers)	Vienna: 11-28-2009 Kiel: 12-13-2009
Trial user selection (members of the built angling community)	Q3 2009
Community field trial kick-off	End of May 2010
Community field trials (system logging, interaction logging, diary)	April 2010
Focus groups (with the participants of the field trials)	End of April 2010
User interviews (with the participants of the field trials)	April 2010

Phase 2	Scheduled
Early prototype testing	Q3 2010
Lab testing (with selected members of the angling community)	Q3 2010

Copyright © 2009 by the PICOS consortium - All rights reserved.

The PICOS project receives research funding from the Community's Seventh Framework Programme.



D7.1a User Evaluation Plan

Phase 2	Scheduled
Field tests (with a number of selected anglers)	Q3 2010
Trial user selection (members of the built angling community)	Q3 2010
Community field trial kick-off	Q4 2010
Community field trials (system logging, interaction logging, diary)	Q4 2010
Focus groups (with the participants of the field trials)	Q4 2010
User interviews (with the participants of the field trials)	Q4 2010



2 Country Report

Main objective of the PICOS project is to research, develop, build, trial and evaluate an open, privacy-respecting, trust-enabling identity management platform that supports the provision of community services by mobile communication service providers.¹ The identity management platform resulting from the PICOS project must respect the laws of the European Community and of the Member States in which it will be used. In order to assist any future deployment of the PICOS project, this report outlines the relevant laws on data protection that will need to be taken into account in two major European Member States, the United Kingdom and Germany. As the PICOS prototype and in future PICOS technology is going to be deployed in various European Member States, we wanted to make an analysis of two countries with different legal system in order to ensure the potential deployment of PICOS throughout Europe. In general the data protection legal frameworks of the European Member States is based on EU Directives and therefore no major differences are found among them. Our country analysis addresses in turn the most pertinent aspects of data protection law in the context of electronic communications networks and services, with a focus on mobile communications, as well as some other relevant law.

In relation to each of these states, this report will address the most pertinent aspects of data protection law in the context of electronic communications networks and services, with a focus on mobile communications, as well as some other relevant law. The regulatory bodies responsible for enforcing the law will also be examined. In order to ensure consistency a common structure has been chosen for the discussion of the legislation of the two Member States.

It should also be noted that data protection law is intimately linked to human rights, especially to Art. 8 of the ECHR: the right to privacy. However, this report is limiting itself to exploring these issues from the micro level of the laws that put these principles into action, rather than at the macro level of the fundamental principles themselves. That should in no way understood as meaning that this report is not concerned with human rights; to the contrary it considers the upholding of human rights to be a fundamental duty of utmost importance.

2.1 *United Kingdom*

2.1.1 Introduction

In the United Kingdom the protection of data is predominantly governed by the Data Protection Act 1998 (c. 29) (DPA),² which implements the Data Protection Directive (DPD)³ into British law, and the

¹ See 4.1 of PICOS D2.3 “Contextual Framework”

² ‘An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information’, 16th July 1998, online at http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1, last checked 7/07/2009

³ ‘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’



Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR),⁴ which implements the E-privacy Directive.⁵ Under the latter rules, a number of more specific issues relating to electronic communications are addressed in more detail, while s.4 of PECR makes it clear that the obligations it imposes are to be interpreted cumulatively with those originating in the DPA. Neither the DPA nor PECR contain provisions mirroring Art. 3(2) of the DPD or Art. 1(3) of the E-Privacy Directive excluding topics such as those covered by Titles V and VI of the Treaty on European Union. The DPA and PECR therefore apply to all data controllers in the United Kingdom as defined s.5 of the DPA.⁶ The Regulation of Investigatory Powers Act 2000 (c. 23) (RIPA)⁷ is also relevant. It regulates all types of interception of communications, and while its primary purpose is to regulate the framework in which the government may monitor its own citizens, it also details under what circumstances private parties may legally intercept communications. Furthermore, a number of other laws not specifically related to data protection, such as the 2006 Fraud Act, are nonetheless relevant to it, and will therefore be discussed. The bodies responsible for enforcing this body of law and their powers will also be detailed.

2.1.1.1 Targeted Advertising systems

An overview of targeted advertising systems is important in the context of the PICOS project, as in a future deployment of the PICOS system; targeted advertising systems may be adopted serving the needs of specific business models. Targeted advertising systems touch upon many aspects of the relevant law and they serve as, and will be used throughout this report as, an informative concrete example of much of the laws potential application. This is particularly useful in a Common Law system such as the UK, where the statutory law alone often forms little more than a skeletal framework to which case-law, and to a lesser degree scholarship, adds flesh. The skeletal nature of the law is especially pronounced in areas such as data protection, which due to their rapid evolution, are necessarily legislated about in a relatively vague fashion. The specific issues that targeted advertising systems raise will be discussed in the appropriate sections.

Official Journal L 281, 23/11/1995 P. 0031 – 0050, online at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

⁴ Statutory Instrument 2003 No. 2426, 18th September 2003, online at <http://www.opsi.gov.uk/si/si2003/20032426.htm>, last checked 7/07/2009

⁵ ‘Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications),’ *Official Journal L 201, 31/07/2002 P. 0037 – 0047*, online at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>

⁶ Section 2.4.2 deals in more detail with who exactly falls within the scope of the DPA.

⁷ ‘An Act to make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; to provide for Commissioners and a tribunal with functions and jurisdiction in relation to those matters, to entries on and interferences with property or with wireless telegraphy and to the carrying out of their functions by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters; and for connected purposes,’ 28th July 2000, online at http://www.opsi.gov.uk/ACTS/acts2000/plain/ukpga_20000023_en, last checked 07/07/2009



D7.1a User Evaluation Plan

There are a number of targeted advertising projects in development that rely on deep packet inspection (DPI) and which have therefore raised privacy concerns. These include KindSight, Experian Hitwise, FrontPorch, Adzilla, Phorm,⁸ and Insight Ready.⁹ However, this report will concentrate mostly on examining the legal ramifications of the Phorm system, rather than other similar systems, as it is by far the most high profile there is already a considerable amount of doctrine surrounding the legality of the technology it employs.

Phorm is normally described as a targeted advertising system,¹⁰ although it seemingly prefers to place an equal, if not greater emphasis, on its capability to supply non-commercial personalised web content.¹¹ In providing both of these services Phorm functions by taking a copy of the information that passes between end-users and websites,¹² which obviously involves the use of the much maligned¹³ Deep Packet Inspection (DPI). Each user is allocated a Unique Identifier (UID), a unique number,¹⁴ which is stored on their computer in a cookie. Phorm's technology then examines their browsing habits in order to determine categories of information in which they are interested, which it calls 'channels.' These are associated with the browser's UID so that advertising can be targeted to the user's interests.¹⁵ The process of matching channels to UIDs, in short, seems to rely on a complex system of 'Chinese walls' within the ISP, whereby information passes between the 'profiler,' 'anonymiser' and 'channel server,' and back again.¹⁶ Phorm claim that their system is entirely anonymous and lacks any means for them to identify their users, as the information related to the user's preferences remains unconnected to their IP address.¹⁷ However, these claims have been disputed by a number of academics¹⁸ and organisations.¹⁹ Phorm has already been trialled in the UK by Virgin Media, TalkTalk and BT, under its Webwise system.²⁰ Since these trials the Phorm system has received considerable press coverage in the UK,²¹ demonstrating that issues of data protection are of considerable public interest in the country.

⁸ NoDPI.org, FAQ, 2009

⁹ Paladine, 'NebuAd pull a fast one!' 2009

¹⁰ Wray, 6th July 2009; Telegraph Staff, 2009; Metz, 2008

¹¹ Phorm, 2009

¹² Clayton, 2008, p.2

¹³ NoDPI.org, 'Welcome to NoDPI, 2009

¹⁴ Clayton, 2008, p. 5

¹⁵ Clayton, 2008, pp. 3-5

¹⁶ For a more detailed explanation of the entire process see, Clayton, R., 'The Phorm "Webwise" System,' 18th May 2008, online at <http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf>, last checked 28/04/2009

¹⁷ Phorm, 2009

¹⁸ Most notably Bohm, in 'The Phorm "Webwise" System – A Legal Analysis,' 23rd April 2008, online at <http://www.fipr.org/080423phormlegal.pdf>, last checked 28/04/2009

¹⁹ For example, NoDPI and Dephormation.

²⁰ Wray, 7th July 2009

²¹ For example, Oates, J, 'Phorm confirms TalkTalk fail,' *The Register*, 8th July 2009, online at http://www.theregister.co.uk/2009/07/08/phorm_talktalk_terminated_confirmed/; Waters, D., 'Phorm – one year on,' *BBC News*, 4th March 2009, online at http://www.bbc.co.uk/blogs/technology/2009/03/phorm_one_year_on.html, last checked 21/08/2009; Charles,



2.1.2 Regulatory bodies and their powers

2.1.2.1 Information Commissioner's Office (ICO)

The Information Commissioner's Office (ICO) is an "independent public body set up to promote access to official information and protect personal information,"²² and it is of course the second part of its mandate with which this report is concerned. It should be noted that in the DPA the ICO is referred to as the Data Protection Commissioner, as it only received its current moniker under the Freedom of Information Act 2000. The ICO is responsible for investigating complaints related to, and enforcing, the DPA and the PECR, as well as issuing guidance in relation to these areas of law. It does this, in respect of the DPA, by maintaining the registry of data controllers provided for in s.19 of the DPA and described below in 'Data controllers' duties', and by acting on 'requests for assessment' submitted under s.42 of the DPA, which allow data subjects to request that the ICO investigate whether a particular data controller is fulfilling their duties. The ICO can issue information notices under s.43 and special information notices under s.44, which oblige the data controller to provide them with information, in response to a 'request for assessment' or of their own volition, in order to investigate whether the data protection principles are being breached. If it believes they are being breached, it can issue enforcement notices under s.40 which require compliance with the DPA.

Art. 31 of the PECR states that s.40 to s.50 of the DPA, which includes the provisions relating to enforcement, shall also apply to the PECR, subject to the modifications in Schedule 1. These modifications remove the possibility of submitting 'requests for assessment', although s.32 allows for a similar mechanism, whereby a data subject can request that the Commissioner exercises his enforcement functions. Schedule 1 also changes references to the data protection principles to references to 'requirements of the PECR'.

In practice it appears that most of the ICO's actions take the form of persuading data controllers to sign formal undertakings that they will respect the data protection principles,²³ which is not a power explicitly given in the DPA, but appears to be a compromise whereby the ICO is assured the law is being respected and the data controller avoids being subject to an enforcement notice. Compared to the equivalent authorities elsewhere in Europe, the ICO is relatively impotent, as it has only weak search powers²⁴. This may explain its reliance on these less formal methods, through which a good relationship with data controllers may be maintained.

Additionally, under s.60 the ICO also has the power to initiate criminal proceedings for offences contained in the DPA. However this is not one of the provisions that are modified for application to the PECR, and so there are no criminal sanctions in relation to these rules, rather s.30 of PECR allows individuals to instigate civil proceedings for breaches of PECR where they have suffered damage, which is not possible under the DPA.

A., 'Phorm fires privacy row for ISPs,' *The Guardian*, 6th March 2008, online at <http://www.guardian.co.uk/technology/2008/mar/06/internet.privacy>, last checked 20/08/2009.

²² ICO, 'Who are we,' 2009

²³ ICO, 'Enforcement,' 2009

²⁴ Korff, 2009, p. 195



The Information Tribunal, which similarly to the ICO is titled the Data Protection Tribunal in the DPA, decides appeals against notices issued by the ICO in relation to the DPA and the PECR.²⁵

2.1.2.2 *The Crown Prosecution Service (CPS)*

The Crown Prosecution Service (CPS), which is headed by the Director of Public Prosecutions (DPP), is the non-ministerial Government Department responsible for prosecuting criminal cases in England and Wales,²⁶ and therefore responsible for prosecuting a number of offences relating to the laws discussed in this report. Particularly important is the fact that it prosecutes offences relating to s.1 of the RIPA (discussed below under section 2.1.8 'Confidentiality of Communications',) s.2 of the Fraud Act, s.60 of the DPA, and offences contained in the SCA such as those relating to incitement.

It is also possible for the DPP to carry out a private criminal prosecution, where a private individual requests that they prosecute and submits the relevant evidence, rather than a public authority, normally the police. Though this happens only occasionally this possibility is relevant to this report, as the DPP is currently deliberating whether to prosecute BT, on the request of NoDPI, for using Phorm without seeking end-user consent,²⁷ as the police found 'no evidence of illegal activity'²⁸ in their investigations, on the basis of either that there was either 'implied consent' or that there was no intent.²⁹

The existence of the Information Commissioner, described in the RIPA as the Interception of Communications Commissioner, should not be allowed to confuse these matters; his responsibilities do not extend beyond supervising the exercise of the various permitted interceptions in the RIPA, by for example the security services, and do not relate to the offence in s.1.

2.1.2.3 *The Home Office*

The Home Office is the ministerial Government Department responsible for law and order. It is responsible for upholding, and reviewing the criminal law and the procedures of the criminal justice system.³⁰ The Home Office, can therefore issue orders, guidance and advice on aspects of criminal law, and has done so in relation to this area, issuing a 'comfort note' to Phorm that states that its technology does not breach RIPA.³¹ While orders are a form of delegated legislation, authorised by the provisions of acts of parliament, and therefore legally binding, the guidance it gives has no legal value, and the Home Office was in the case of its advice to Phorm at pains to make this clear.³²

²⁵ Information Tribunal, 2009

²⁶ CPS, 2009

²⁷ Paladine, 'Off to Brussels,' 2009

²⁸ Johnson, 2008

²⁹ European Commission, "Progress Report on the Single European Electronic Communications Market 2008 (14th Report)," 2009, p. 346

³⁰ CPS, 2009

³¹ Home Office, 2008

³² Home Office, 2008, at 2



2.1.3 Personal Data

2.1.3.1 Definition

Personal data is defined in s.1 (1) of the DPA as “data which relates to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual”. Notably, unlike in the DPD, data itself is also defined in the same article.³³ Although this might appear to be a ploy to narrow the definition of personal data, which technically it does, its main function appears to be stylistic; British laws tend not to include an Article on scope, as most directives do, and so instead the limits of the law’s reach are delimited by more restrictive definitions. Here there is a clear manifestation of this phenomenon; the definition of data is substantively almost identical to s.3 of the DPD on ‘Scope.’ Therefore the DPA, save for issues of territoriality, applies to all processing of personal data fulfilling the above definition.

2.1.3.2 Interpretation

Although this definition of personal data differs considerably from that in Article 2(a) of the DPD as discussed in section 4.2.1 of PICOS D2.3 “Contextual Framework”, it appears to be considered, by the Information Commissioners Office, to mean essentially the same thing.³⁴ This is however a questionable assertion, as although the basic substance, that it is data which allows an individual to be identified, is the same, there is no explicit mention of identification numbers or “factors specific to his/her physical, physiological, mental economic, cultural or social identity.” Since the DPD states that personal data may be identified “in particular” by reference to these things, it would appear to have been useful to include these in the DPA as they are not merely illustrative examples, but rather categories of information that the European legislature clearly intended to constitute personal data. The omission of this part of the DPD’s definition in the DPA therefore suggests that perhaps the concept of personal data in the UK is narrower than in the DPD. The Court of Appeal’s approach in *Durant v. Financial Services Authority*,³⁵ appears to confirm this supposition, as it made clear that not all data that can be “retrieved from a computer search against an individual’s name or unique identifier is personal data within the Act. Mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data.”³⁶ It goes on to explain that in determining if something does constitute personal data, both whether data is biographical in a significant sense, meaning it concerns, “a life event in respect of which his privacy could...be said to be compromised,” and the data’s “focus,” which for personal data is the putative data subject, are indicative. According

³³ In s.1 (1) of the DPA data is defined as being; “information which (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68; or (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)”

³⁴ ICO, 2007, p. 3

³⁵ [2003] EWCA Civ 1746

³⁶ [2003] EWCA Civ 1746, at 28



D7.1a User Evaluation Plan

to the ICO the judgment is based on the rather tortuous logic that although the data subject is identifiable in situations like this, since the data includes their name, the data does not “relate to” them.³⁷ However, the interpretation of personal data espoused in *Durant* has since been confirmed by the courts’ in *Johnson v MDU*³⁸, in which it was held that not all documents referring to Dr. Johnson ‘related’ to him and that therefore some of them did not constitute personal data and in *Smith v Lloyds TSB*³⁹, in which it was held that though documents held by Lloyds TSB referred to Mr Smith they were not personal data, as they ‘related’ to the company of which he was managing director, rather than him⁴⁰.

This narrow interpretation is at odds with the more common European approach to personal data, which conceives of it broadly, and as Kuner states, even treats the burden of proof as being on the controller to show that it is not personal⁴¹. It is therefore unsurprising that it has come under considerable criticism, by for example Lorber⁴², who states that it “puts considerable strain on the statutory framework, quite possibly rendering the UK in breach of its obligations to transpose the Directive,” and Dr. Pounder⁴³ who describes how it has led to data controllers, in his view mistakenly, understanding *Durant* as containing additional criteria which must be fulfilled for data to qualify as personal data. Lorber’s opinion was shown to be justified as the European Commission exchanged letters with the Ministry of Justice, in which it questioned whether 11 Articles of the DPD, including the definition of personal data, were properly implemented.⁴⁴ However the European Commission does not appear to have initiated any proceedings against the UK in relation to this specific issue.⁴⁵ Lorber suggests that the Ministry of Justice succeeded in persuading the Commission that *Durant* was being misinterpreted by data controllers as prescriptive, when the Court had in fact only meant them to be “helpful,”⁴⁶ and therefore the actual law was not in breach of the Data Protection Directive.

Where data is not recorded on a computerised system, meaning “equipment operating automatically in response to instructions given for that purpose,”⁴⁷ it may still be considered data, and in turn personal

³⁷ ICO, ‘*The ‘Durant’ Case and its impact on the interpretation of the Data Protection Act 1998,*’ 2006, p. 2

³⁸ 2004 EWHC 347

³⁹ 2005 EWHC 246

⁴⁰ The ICO’s interpretation of what amounts to personal data is set out comprehensively, with practical examples, in, Information Commissioner’s Office, ‘*Data Protection Technical Guidance Determining what is personal data,*’ 21st August 2007, online at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flow_chart_v1_with_preface001.pdf, last checked 28/04/2009

⁴¹ Kuner, 2003, p. 51

⁴² Lorber, 2004, p. 189

⁴³ ‘House of Lords ends Durant’s data protection saga,’ 2005

⁴⁴ ‘Europe claims UK botched one third of Data Protection Directive,’ 2007

⁴⁵ However, as is discussed above, the European Commission has launched an investigation into the implementation of the DPD in the UK. This investigation appears to be focussed on whether projects such as Phorm are obeying the Data Protection Principles, rather than whether the definition of personal data is compliant with the DPA.

⁴⁶ ‘House of Lords ends Durant’s data protection saga,’ 2005

⁴⁷ Art. 1(3) DPA.



data, if it forms part of a “relevant filing system.”⁴⁸ Exactly what constitutes a relevant filing system is also dealt with in detail in the *Durant* judgement. To qualify as a relevant filing system it must provide the “same standard or sophistication of accessibility to personal data...as [in] computerised records,”⁴⁹ and be “broadly equivalent to [a] computerised system.”⁵⁰ Furthermore, a system will only be a relevant filing system if “the files forming part of it are structured or referenced in such a way as clearly to indicate at the outset of the search whether specific information capable of amounting to personal data of an individual...is held within the system and, if so, in which file or files it is held”⁵¹ and if it “has as part of its own structure or referencing mechanism, a sufficiently sophisticated and detailed means of readily indicating whether and where in an individual file or files specific criteria or information about the applicant can be readily located.”^{52,53}

2.1.3.3 Sensitive personal data⁵⁴

This subcategory of personal data is defined in s. 2 of the DPA as consisting of information as to the racial origin of the data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, whether he is a member of a trade union, his physical or mental health or condition, his sexual life, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. The use in the DPA of the phrase “as to” in reference to what constitutes sensitive personal data does, as Korff points out, suggest a narrower conception of such data than the use for example of “reveal,” which has been used in transposing the DPD in several Member States.⁵⁵ For instance, data that records that someone buys kosher meat may not be data as to their religious beliefs, but it may reveal them.⁵⁶

The classification of data as sensitive personal data, rather than merely personal data, is significant, as it has profound effects on the conditions under which it may be processed. This is discussed in detail in section 2.1.4.14 of this report.

2.1.3.4 IP Addresses

The issue of whether IP addresses constitute personal data within the meaning of Art. 2(a) of the DPD has already been discussed in some detail in section 6.4 of PICOS D2.4 “Requirements,” and the question of whether IP addresses relate to an identified or identifiable natural person remains an

⁴⁸ *ibid*

⁴⁹ [2003] EWCA Civ 1746, at 34

⁵⁰ *ibid*, at 47

⁵¹ *ibid*, at 50

⁵² *ibid*, at 50

⁵³ The ICO’s interpretation of what amounts to a relevant filing system is set out comprehensively, with practical examples, in, Information Commissioner’s Office, ‘*Data Protection Technical Guidance Determining what is personal data*,’ 21st August 2007, online at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flow_chart_v1_with_preface001.pdf, last checked 28/04/2009

⁵⁴ In the DPD, and Germany, this data is described as consisting of ‘special categories of personal data.’

⁵⁵ Korff, 2002, p. 82

⁵⁶ *ibid*



D7.1a User Evaluation Plan

extremely contentious issue. While views such as the Article 29 Working Party's repeated assertions that IP addresses do constitute personal data and the Paris Court of Appeals recent decisions to the contrary,⁵⁷ should be borne in mind, in the context of UK law they are by no means authoritative. There is no UK case-law that authoritatively settles this issue but the ICO has issued guidance that states that it depends on the type of IP address. It states that static addresses probably do constitute personal data, as they can be linked to an individual user or at least a particular computer, while dynamic ones do not.⁵⁸ This guidance is only intended for processors of IP addresses other than the ISPs themselves, a category in which researchers working for the PICOS project would presumably fall. Conversely, it appears to imply that ISPs processing IP addresses are processing personal data, as they have the necessary information to link ISPs to users, though there is no explicit statement to this effect.⁵⁹

In addition to the ICO's advice it seems prudent to keep in mind the original provisions of the DPA and the DPD which hinge on whether or not the information enables the identification of an individual, and to apply this to the particular situation at hand. This case by case approach is supported by Article 29 Working Party and the European Data Protection Supervisor.⁶⁰ However, these matters should be monitored carefully in case there are any developments that further clarify the status of IP addresses in the UK.

The discussions surrounding targeted advertising systems add another level of complexity to this debate,⁶¹ as they raise the issue of whether the cookies containing UIDs used in targeted advertising systems to identify users constitute personal data. It seems likely that they do as the placing of a UID on a user's computer is analogous to a static IP address, as it is a number permanently, or at least for a time, associated with a particular computer it would therefore be, in accordance the ICO's advice, personal data.

The interplay between IP addresses and cookies containing UIDs is also interesting, as it raises questions about what can constitute the "other information which is in the possession of, or is likely to come into the possession of, the data controller" in the definition of personal data in s.1 (1) of the DPA, which allows a person to be identified or to become identifiable in conjunction with the putative personal data. It appears that IP addresses would be more likely to be personal data when in the possession of a data controller who also has access to, or is likely to get access to UIDs, as the channels indicating the users interests that these contain could be the additional information that would allow an individual to be identified. For example where a family shares an IP address, if it were not to be considered personal data as it does not indicate which family member is using the computer, were it to be a computer that stored cookies separately for each user then the combination of the IP address and the UID could identify a family member, since there might only be one member who for example

⁵⁷ Section 6.4 of PICOS D2.4 "Requirements" explores these views in more detail.

⁵⁸ ICO, 5th June 2007, p. 3

⁵⁹ ICO, 5th June 2007, p. 3. The phrase that appears to imply this states; "it is only the ISP who can link the IP address to an individual."

⁶⁰ Section 6.4 of PICOS D2.4 "Requirements," p. 96

⁶¹ It is notable that Phorm appear to be concerned that IP addresses do constitute personal data, as in their meeting with Richard Clayton they stated that the reason that a 'channel server' is located within each ISP, rather than there being a single centralised one, is that they were concerned they might breach rules about moving personal data outside Europe.(Clayton, 2008, p. 8)



liked fishing. The Phorm system, for example, would perhaps encounter legal hurdles in this area as although Phorm does not envisage any linkage of IP addresses and UIDs,⁶² and has gone to some lengths to construct an architecture within the ISP that prevents this from happening, this is without legal significance. There would still be the possibility that the UID and the IP address could together be used to identify an individual, and that is enough for either of those things to qualify as personal data.

2.1.4 Processing of Personal Data

2.1.4.1 Definition

Art. 1(1) of the DPA defines ‘processing in relation to information or data’ as ‘obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including,

- (a) organisation, adaptation or alteration of the information or data,
- (b) retrieval, consultation or use of the information or data,
- (c) disclosure of the information or data by transmission, dissemination or otherwise making available,
- or (d) alignment, combination, blocking, erasure or destruction of the information or data.’

This definition, like that in the DPD⁶³, is clearly very broad; it is very difficult if not impossible to think of operations that do not constitute, ‘processing.’ There is even an argument the UK definition is broader, as ‘holding,’ appears to encompass both long term and very short term retention of data, while ‘storage’ arguably does not connote short term retention.

2.1.4.2 Relevant parties

The DPA in s.1(1), like the DPD, distinguishes three groups for the purposes of regulating data processing, which are;

“data controller” means, subject to subsection (4)⁶⁴, a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;

“data processor” in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

“data subject” means an individual who is the subject of personal data.

⁶² Clayton, 2008, p.9

⁶³ Art. 2(b) of the DPD states that processing “shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.”

⁶⁴ Subsection (4) merely clarifies that where a party is statutorily obligated to process data they remain the ‘data controller.’



This provision does not explicitly state, as its equivalent in the DPD does, that ‘a person’ means both legal and real persons, but this certainly does not indicate that it does not apply to both categories, which following the established use of ‘persons’ under UK law it clearly does.

Who qualifies as a data controller is further elaborated upon in s.5 of the DPD which states that the DPA applies to any data controller either established in the United Kingdom when the data are processed in the context of that establishment, or established neither in the United Kingdom nor in any other EEA State but who uses equipment in the United Kingdom for processing the data otherwise than for the purposes of transit through the United Kingdom. A data controller is established in the UK if they are ordinarily resident in the United Kingdom, a body incorporated under the law of, or of any part of, the United Kingdom, a partnership or other unincorporated association formed under the law of any part of the United Kingdom, or if they maintain in the United Kingdom a regular practice, or an office, branch or agency through which they carry on any activity.

As ‘Section 2.1.4.3 Data controllers’ duties’ below shows, the responsibility for conforming to the law falls on the data controller and not the data processor. In the case of targeted advertising technologies such as Phorm, Bohm maintains that the ISP employing the technology is the data processor,⁶⁵ while the software developer probably is not even a ‘data processor,’ although if the ‘channel server’ were under their control rather than the ISP’s they would be.

2.1.4.3 Data controllers’ duties

The delineation of parties is crucial, as s. 4 (4) of the DPA, states that it “shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller”. Failure to do so can lead to the intervention of the ICO, and the eventual imposition of penalties under s.60, if the ICO’s notice is not complied with. In the case of breaches of PECR, it can also render the data controller civilly liable to injured parties.⁶⁶

Furthermore, Part III, specifically s.17 read in conjunction with s.16 and 18, obliges data controllers to register with the ICO, to whom they must notify a relatively extensive set of information, including their name and address, descriptions of the data to be processed, the purpose of the processing and any intended recipients, before they process data.⁶⁷ S.21 makes it an offence not to do so, for which the data controller may be fined in accordance with s.60.

However, according to s.17 this prohibition on processing without notification, does not apply where the processed information’s sole purpose is the keeping of a public register, or if it is only part of a relevant filing system, or if it falls within the scope of a notification regulation that the Secretary of State has issued decreeing “that processing of a particular description is unlikely to prejudice the rights and freedoms of data subjects”⁶⁸. The Secretary of State’s power here can be understood as analogous to that of the European Commission regarding block exemptions in competition law, as it can by regulation relieve qualifying groups from regulatory obligations. However no such regulations yet

⁶⁵ Bohm, 2008, p. 13

⁶⁶ S.30 of PECR

⁶⁷ The online notification form through which data controllers are obliged to notify the ICO that they are processing data can be found at <https://forms.informationcommissioner.gov.uk/cgi-bin/dprproc?page=7.html>

⁶⁸ S.17 DPA



exist.⁶⁹ Furthermore, Part IV of the DPA declares that these duties of notification do not apply to data processing related to national security in s.28 and performed for domestic purposes in s.36, but crucially for PICOS no such exemption is found in s.33 which concerns research history and statistics.

2.1.4.4 Data protection principles

The description of the basic principles and their ideological underpinnings found at 4.2.2 of PICOS D2.3 “Contextual Framework,” will not be repeated here; rather the UK’s interpretation of them will be examined. Therefore only the aspects of UK’s transposition of the DPD which are worthy of note will be addressed; less significant parts of the DPD that have been implemented verbatim will not be. Overall it will be demonstrated that the UK’s implementation tends to the lax, offering less data protection than in perhaps found in other countries⁷⁰, and therefore making the duties to which data controllers are subject less burdensome.

The principles that data controllers are bound to apply when processing personal data are laid out in Part I of Schedule 1, and are elucidated in Part II of Schedule 1 of the DPA, as Article 5 of the DPD requires when it states “Member States shall...determine more precisely the conditions under which the processing of personal data is lawful.” These consist of the principles ‘relating to data quality’ found in Art. 6 of the DPD as well as the requirements relating to ‘security of processing’ in Art.17, while the ‘criteria for making data processing legitimate’ of Art. 7 of the DPD are found in Schedule 2, which in the DPA, unlike the DPD, is explicitly linked to the first data protection principle: that data be “processed fairly and lawfully.” This results in at least one of the conditions in Schedule 2 having to be met for data processing to be fair and lawful. The conditions that make the processing of sensitive personal data lawful, which are found in Art. 8 (2) - (5) of the DPD, and in Schedule 3 of the DPA are also formally linked to the first principle, so that for the processing of sensitive data to be fair and lawful, a criterion from both Schedule 2 and 3 must be fulfilled.⁷¹ Additionally, Section IV of Chapter II of the DPD, on ‘information to be given to the data subject,’ is included in Part II of Schedule 1 of the DPA, as another necessary condition of the first data protection principle.

These duties apply to all ISPs as a considerable amount of the information that an ISP processes, in the sense of transmits, is data from which a living individual can be identified, especially when it is combined with the other information that the ISP holds about who pays for the internet connection. Data concerning logging into an email or social-networking account is a particularly obvious example of such personal data. Further, much of what an individual looks at on the internet, qualifies as sensitive personal data, since it might relate to their political views or sexual life etc. ISPs employment of targeted advertising technology is a separate processing action that also, as it involves inspecting nearly all internet traffic, some of which is bound to constitute personal data as well as sensitive personal data, must be performed in compliance with the data protection principles. The fact that this processing, is entirely automatic, takes place very quickly, and apparently leaves no evidence, from which an individual could be identified, does not exclude it from the ambit of the DPA. As Bohm says, brevity is no defense⁷².

⁶⁹ ICO, 2001, p. 98

⁷⁰ Korff, 2002, p. 61

⁷¹ See Section 2.1.4.14, ‘Processing sensitive personal data.’

⁷² Bohm, 2008, p. 13



2.1.4.5 First data protection principle

The first principle's application is somewhat limited in the UK as it is assumed the processing is fair and lawful if the data is "obtained from a person who...is authorised by or under any enactment to supply it...or is required to supply it by or under any enactment."

The UK's implementation of the Section IV of Chapter II of the DPD as a condition for fulfilment of the first principle, in s.2 (1)(a) of Part II of Schedule 1 of the DPA, introduces a criterion of practicability; data controllers must only provide the data subject with the 'relevant information' where it is practicable to do so. The 'relevant information' consists of: the identity of the data controller and if applicable his representative, the purposes for which the data are intended to be processed, and any further information which is necessary, having regard to the specific circumstances, to enable processing in respect of the data subject to be fair. This applies both to data harvested directly from data subjects and data gathered by other means, and in the latter's case the time limit within which the subject must be informed is also tempered by the condition of practicability. Art. 11 (2) of the DPD does, slightly analogously, state that the 'relevant information' need not be given where it would involve disproportionate effort. However, unlike the practicable caveat, the exception for a disproportionate effort only applies to information which is not gathered from the data subject, and further is limited largely to the case of "processing for statistical purposes or for the purposes of historical or scientific research"⁷³. Furthermore, the disproportionate effort exception for data not gathered from the data subject is also preserved in the DPA in s.3 (2) (2) (a) of Part 1 of Schedule 1, although the limitation that it applies predominantly in the case of historical or scientific research is not. Overall the duties of Section IV of the DPD seem to be less burdensome in the UK, and in the opinion of Bainbridge and Pearce, are not even properly implemented.⁷⁴

As it has been stated, the principles contained in the DPD that render data processing legitimate have been incorporated in Schedule 2 of the DPA, as criteria that indicate whether the first principle is being adhered to; at least one must be fulfilled. Furthermore the ICO has made it clear that they all carry equal weight, and that the order in which they appear in the act is not indicative of anything.⁷⁵

The data subject's consent, which is one of the possible justificatory criteria, is not defined at any point in the DPA, which it is in Art. 7 (a) of the DPD. This obviously leaves its meaning rather more protean, especially as the ICO says only of the DPD definition that it may be helpful, not that it is in any way authoritative.⁷⁶ Whether this means implied consent qualifies as consent under the UK law is the subject of much discussion, though the ICO has stated that consent may not be inferred from complete non-response.⁷⁷ It can be argued that since the phrase "explicit consent" is used in Schedule 3, in relation to the processing of sensitive data, that unless sensitive data is concerned the consent need not be explicit, and therefore can be implied.⁷⁸ The DPD clearly states that the data subject's consent needs to "be signified," and while Korff seeks to reconcile the DPD and the DPA by

⁷³ Bainbridge and Pearce, 2000

⁷⁴ Bainbridge and Pearce, 2000

⁷⁵ ICO, 2001, p. 29

⁷⁶ ICO, 2001, p. 29

⁷⁷ ICO, 2001, p. 29

⁷⁸ Korff, 2002, p. 71



suggesting there is a third category where consent is not explicit but it is otherwise signified,⁷⁹ it is perhaps better just to accept that the DPA fails to implement the DPD effectively in this regard.

Schedule 2 makes it clear that data processing will also be legitimate if “the processing is necessary...for the performance of a contract to which the data subject is a party, or...for the taking of steps at the request of the data subject with a view to entering into a contract”, or to comply with any legal obligation, other than a contractual one, to which the data controller is subject, or to protect the vital interests of the data subject, or for the administration of justice, or for the exercise of any functions conferred on any person by or under any enactment or for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or for the exercise of any other functions of a public nature exercised in the public interest by any person.

Finally, data processing may also be legitimate if, under s.6 of Schedule 2 of the DPA “the processing is necessary for the purposes of legitimate interests pursued by the data controller...except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.” This criterion allows the interests of the data subject and controller to be balanced, and it is notable that the Home Secretary may by order specify particular circumstances in which it is automatically met, although this does not appear to have yet happened. Though, the ICO has stated they will take a broad view of legitimate interests.⁸⁰

ISPs’ processing of personal data, in the sense of transmitting it, is clearly fair and lawful as they are processing it in order to fulfil their contract with the data subject, and additionally this contract also operates to give them consent to do so. However, their processing in the context of targeted advertising systems is might not be fair and lawful. It is unlikely that they are under a contractual obligation to the data subject to do this, and whether they have consent is obviously dependant on whether implied consent is considered valid, unless they employ the technology on an opt-in basis which Phorm certainly didn’t in the secret trials of 2006/2007. It is also possible that ISPs using a targeted advertising system would be able to rely on s.6 of Schedule 2.

It is also important to remember that, regardless of the criteria discussed, processing can self-evidently not be lawful if it involves the breach of a law,⁸¹ and so if targeting advertising technology is in breach of one of the other laws discussed in this report, such as the Fraud act or RIPA it will also be in breach of the first data protection principle.

2.1.4.6 Second data protection principle

Part II of Schedule 1 of the DPA makes it clear that the second principle’s requirement that the data be processed for a specified purpose can be fulfilled by a specification either in the information given to the data subject, or in the notification sent to the ICO. The pro forma notification form contains rather general standard purposes such as “consultancy and advisory services,”⁸² demonstrating that this is not a particularly onerous requirement. Further the ICO pays scant attention to enforcing the second aspect

⁷⁹ Korff, 2002, p.71

⁸⁰ ICO, 2001, p. 20

⁸¹ R v R [1991] 4All ER 481 confirms that whether something is lawful or unlawful follows the natural meaning of unlawful has been broadly described by the Courts as “something which is contrary to some law or enactment or is done without lawful justification or excuse”.

⁸² ICO, ‘Online notification form,’ 2009



of the second principle, that data is not processed in a manner incompatible with the original purpose for which it was gathered.⁸³ Part II of Schedule 1 of the DPA also states that to determine “whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.”⁸⁴

Importantly for projects such as PICOS, s.33 (2) which is concerned with processing for research purposes, states that, “for the purposes of the Second Principle, the further processing of personal data in compliance with the conditions set out in section 33 of the Act is not to be regarded as incompatible with the purposes for which they were obtained”⁸⁵. These conditions require that that “the data are not processed to support measures or decisions with respect to particular individuals, and that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject. It should be noted that the word ‘substantial’ makes this what Korff describes as a weighted balance test”⁸⁶, whereby the individuals’ interests must be balanced with the benefits of the research, and therefore some adverse effects for individuals are legitimate.

However it does seem that a system such as Phorm’s would breach the second principle, depending on the interpretation given to the word incompatible, which as Korff states is inherently vague.⁸⁷ Certainly if it was given the interpretation it is given in other countries, that it means processing within the ‘reasonable expectations of the data subjects,’ then it seems that a covert targeted advertising system, such as Phorm in the context of the 2006/2007 trials, would be in breach of it.

2.1.4.7 Third data protection principle

*The third principle states that, “personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.” These requirements are obviously somewhat vague, especially as Part II of Schedule 1 does not elaborate further. However the ICO has published guidance on what it means, stating that “data controllers should seek to identify the minimum amount of information that is required in order properly to fulfil their purpose, [which] will be a question of fact in each case,”⁸⁸ and not collect more information than this. *The Data Protection Tribunal in Community Charge Registration Officer of Runnymede Borough Council v. Data Protection Registrar*,⁸⁹ makes it clear that where a property type information is held about a larger number of individuals than it will be useful in relation to, it is a breach of the third principle to retain the unnecessary information. Although this case concerns the predecessor to the DPA, the ICO treats it as authoritative in its guidance.⁹⁰ The guidance also states that information can only be held on the*

⁸³ Korff, 2002, p. 65

⁸⁴ ICO, ‘Online notification form,’ 2009.

⁸⁵ S.33(2) DPA

⁸⁶ Korff, 2002, p. 66

⁸⁷ Korff, 2002, p.62

⁸⁸ ICO, 2001, p. 36

⁸⁹ Case DA/90 24/49/3

⁹⁰ ICO, 2001, pp. 36-37



basis that it might possibly be useful in the future if it is known how it would be used, and that keeping data for longer than necessary would likely be irrelevant and excessive.⁹¹

2.1.4.8 Fourth data protection principle

The concept of accuracy in the fourth principle is limited under the UK law, as inaccurate information is defined in s.70 (2) as only being that which is “incorrect or misleading as to any matter of fact”, which unlike the laws of other Member States⁹² obviously excludes any substantive assessments, despite how damaging they can be, if for example they state an individual is a terrible employee. Further, in Part II of Schedule 1 it is made clear that rather than correcting information, where data controllers have taken reasonable steps to ensure it is accurate and sufficient, when data subjects dispute the accuracy, to merely modify the data so it indicates that fact. The ICO has indicated that here reasonable steps means that data controllers must take steps to ensure the accuracy of the data themselves, even where data was obtained from either the data subject or a third party. It goes on to say “the extent to which such steps are necessary [is] a matter of fact in each individual case and will depend upon the nature of the data and the consequences of the inaccuracy for the data subject.”⁹³

The second part of the fourth principle states that where necessary data must be kept up to date, and in deciding the question of whether it is necessary the ICO indicates that the following factors are relevant; whether there is a record of when the data were recorded or last updated, whether all those involved with the data are aware that the data do not necessarily reflect the current position, whether effective steps are taken to update the personal data and whether the personal data being out of date is likely to cause damage or distress to the data subject.⁹⁴

2.1.4.9 Fifth data protection principle

Crucially for research projects such as PICOS, s.33 (3) of the DPA states that “personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle, be kept indefinitely,” and therefore the fifth principle which states that “personal data shall not be kept for longer than is necessary,” is largely irrelevant to such projects.

However in situations where the ‘relevant conditions’ have not been fulfilled because either the data are processed to support measures or decisions with respect to particular individuals, or the data are processed in such a way that substantial damage or substantial distress⁹⁵ is, or is likely to be, caused to a data subject, the ICO guidance on the subject is still relevant. This suggests that data controllers review what personal data they are processing regularly and delete the data which are no longer required for their purposes.⁹⁶ The ICO also draws particular emphasis to the importance of such reviews when the relationship between the data controller and data subject ends or changes, as, for example, when a contract of employment ends.⁹⁷ This is not to be understood as meaning that no

⁹¹ ICO, 2001, p. 37

⁹² Korff, 2002, p. 61

⁹³ ICO, 2001, p. 38

⁹⁴ ICO, 2001, p. 38

⁹⁵ See also section 2.4.4.2 above

⁹⁶ ICO, 2001, p. 39

⁹⁷ ICO, 2001, p. 39



information can be retained once a relationship is over, as it might of course be necessary to provide references for the employee in the future or to defend legal claims.

2.1.4.10 Sixth data protection principle

The sixth data principle states that personal data shall be processed in accordance with the rights of data subjects under this Act. It is the corollary of the rights given to data subjects in Part II of the act, discussed below in Section 2.1.7 ‘Rights of the data Subject,’ in that it makes it clear that data controllers must respect these rights. In Part II of Schedule 1 it is stated that the sixth principle will be breached if, the data controller fails to supply information in accordance with s.7, fails to comply with a notice given under s.10 (1) to the extent that the notice is justified, or fails to comply with a notice given under s.11 (1), s.12(1) or s.12 (2)(b), or fails to give a notification under subsection s.10 (3), or.12 (2)(a).

It is important to note that the above are the only ways this principle can be breached. S.33 (4) further states that personal data processed only for research purposes are exempt from section 7, as long as “the data are not processed to support measures or decisions with respect to particular individuals”, “the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject” and “the results of the research or any resulting statistics are not made available in a form which identifies data subjects”. Therefore a research project such as PICOS, if these conditions were fulfilled, would not be considered to be in breach of the sixth principle because it ignored a s.7 request.

2.1.4.11 Seventh data protection principle

The seventh principle, which is based on Art.17 of the DPD, states that, “appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”. This is a very broad principle that covers the deployment of a huge range of practical measures which cannot all be explored here; only those specifically mentioned in the act and the more significant of those in the ICO guidance will be outlined.

Part II of Schedule 1 explains that in determining what an appropriate level is the following factors should be taken into account; the state of the technological development of possible protective measures, the cost of possible protective measures, the nature of the data and the degree of harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage of the data. It also obliges data controllers to take the organisational measure of taking reasonable steps to ensure the reliability of employees who have access to personal data.

Furthermore it states that relationships between data processors and data controllers must be governed by a written contract, which gives the data processor no opportunity to process the data other than at the data controller’s behest, and specifically obliges adherence to the data protection principles. Data controllers must only select data processors “providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out”.

The ICO encourages data controllers to follow the three step methodology of, identifying potential threats to the system, examining the vulnerability of the system to those threats and putting into place appropriate counter-measures to reduce and manage the risk. In doing this the ICO suggests data controllers examine, whether the organisation has a security policy, if sufficient resources and



facilities are made available for security measures, whether physical access to buildings or rooms containing personal data is controlled, whether passers-by can read information off screens or documents, whether passwords are kept private and changed regularly, whether there is a procedure for cleaning media (such as disks) before they are reused, whether printed material is disposed of securely, whether there is a secure procedure covering the temporary removal of personal data from the data controller's premises, for example, for staff to work on at home, whether data is backed up responsibly.⁹⁸

When employing or promoting staff the ICO says data controllers should give proper weight to the discretion and integrity of staff and that staff should be given adequate training, be made aware of their responsibilities. If employees breach the data protection principles the ICO avers that they should be disciplined and have their access to personal data withdrawn.⁹⁹

The ICO's complete guidance¹⁰⁰ is very informative and in complying with the Seventh Principle it is also well worth making reference to the [International Organisation for Standardisation's](#) (ISO) standards in relation to these matters, namely, 'ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk,¹⁰¹ and the 'ISO/IEC 27002:2005 Code of Practice for Information Security Management'¹⁰². In the UK compliance with these standards can be accredited by an appropriate body, meaning one approved by the UK Accreditation Service (UKAS).¹⁰³

It is also important to note that the general objective that this principle pursues, that personal data should be processed in a secure environment, is not only supposedly realised through this principle but also through s.5 and 6 of the PECR.

2.1.4.12 Eighth data protection principle

The Eighth principle requires that personal data should only be transferred outside the European Economic Area to countries or territories which ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. This principle will not be further elaborated, as for the needs of the PICOS project, the data will not leave the EU.

2.1.4.13 Exemptions

Part IV of the DPA describes many categories of data processing, such as that being performed in the interests of journalism, literature, art¹⁰⁴ or national security¹⁰⁵ that are exempt from the data protection

⁹⁸ ICO, 2001, p.40-43

⁹⁹ ICO, 2001, p.42

¹⁰⁰ Information Commissioner's Office, 'Data Protection Act Legal Guidance' 2001, online at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf, last checked 9/07/2009

¹⁰¹ ISO, 2008

¹⁰² ISO 2005

¹⁰³ Department for Business Information and Skills, 2009

¹⁰⁴ S.32 of the DPA



principles to varying degrees. Of particular concern to this report is s.33, which deals with data processing for research, historical and statistical purposes. The exemptions it provides for in relation to the fifth principle, the second principle, and the sixth principle are detailed above in the principle's respective sections.

It should also be added that s.33 of the DPA makes it clear that these exemptions will still apply if the data are disclosed,

“(a) to any person, for research purposes only;

(b) to the data subject or a person acting on his behalf,

(c) at the request, or with the consent, of the data subject or a person acting on his behalf,

or

(d) in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within paragraph (a), (b) or (c)”.

2.1.4.14 Processing sensitive personal data

According to s. 4(3) and Principle 1, of Part 1, of Schedule 1 of the DPA, which transposes Art. 8 (2) – (5) of the DPD, sensitive personal data may only be processed if one of the conditions in Schedule 3, as well a condition from Schedule 2, is met. This is again a requirement that must be met in order for the processing to be fair and lawful under the first data protection principle. Schedule 3 is more stringent than Schedule 2 and also far more detailed. The PICOS project, in the scheduled applications, will not process any sensitive data. However, in any research project it may be the case that data will be encountered concerning, for example, a data subjects political opinions or religious beliefs. Therefore the conditions which render the processing of sensitive personal data legitimate will be briefly outlined.

The ten conditions which can render the processing of sensitive data legitimate, as long as a condition from Schedule 2 is also met, are, briefly;

1. The data subject has given his explicit consent to the processing of the personal data.
2. The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
3. The processing is necessary in order to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of, or reasonably be expected to be obtained from, the data subject, or in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
4. The processing
 - (a) is carried out in the course of its legitimate activities by any body or association which—
 - (i) is not established or conducted for profit, and

¹⁰⁵ S.28 of the DPA



D7.1a User Evaluation Plan

- (ii) exists for political, philosophical, religious or trade-union purposes,
 - (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
 - (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
 - (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
 6. The processing is necessary for the purpose of any legal proceedings, obtaining legal advice, or in order to establish, exercise or defend legal rights.
 7. The processing is necessary for the administration of justice, for the exercise of any functions of either House of Parliament, or for the exercise of any functions conferred on any person by or under an enactment, or for the exercise of any functions of the Crown.
 - 7a The processing is in connection with the operations of an anti-fraud organisation.
 8. The processing is necessary for medical purposes and is undertaken by a health professional, or someone owing an equivalent duty of confidentiality.
 9. The processing is of sensitive personal data relating to racial or ethnic origin, is being used for equality mentoring.

Furthermore, of vital importance to projects such as PICOS is the fact that Schedule 3 also makes it possible for the Secretary of State to issue an order specifying in more detail the circumstances in which it is lawful to process sensitive personal data which he has done: The Data Protection (Processing of Sensitive Personal Data) Order 2000.¹⁰⁶ This outlines ten such contexts, five of which require that the processing be “in the substantial public interest.” The first of these is research, which must come as a relief for researchers as while some exceptions in Part IV of the DPA do apply to sensitive personal data, such as national security and in certain circumstances journalism, literature and art, research does not. The other four are; processing to prevent or detect unlawful acts where seeking the consent of the data subject would *prejudice* that aim, processing to protect members of the public from certain often lawful but also harmful conduct such as incompetence or mismanagement, where seeking the consent of the data subject to the processing would prejudice those purposes, processing involving the provision of confidential counseling, advice, support or other service, on condition that the data subject cannot consent, or that the controller cannot reasonably be expected to obtain the data subject’s consent, or where obtaining the data subject’s consent would prejudice the provision of that counseling and finally whistleblowing. Whistleblowing meaning disclosures of personal data that are in the public interest as they reveal unlawful acts, dishonesty, malpractice or other seriously improper conduct, often on the part of members of the government.¹⁰⁷

¹⁰⁶ Statutory Instrument 2000 No. 417, 17th February 2000, online at <http://www.opsi.gov.uk/si/si2000/20000417.htm>, last checked 9/07/2009

¹⁰⁷ Korff, 2002, pp. 88-89



This “substantial public interest” criterion is probably not as strict as it first appears. The ICO has for example stated that keeping records of employee sickness is a matter of “substantial public interest.”¹⁰⁸ Therefore it seems that the broad and relatively numerous additional circumstances in which sensitive personal data may be processed, enunciated in the Order, have substantially weakened the protection of sensitive personal data, and made the job of data controllers, including those involved in research, easier. Data controllers involved in research can process sensitive personal data, if it is in the substantial public interest, though the additional criteria that it does not support decisions about a particular data subject otherwise than with their explicit consent and that it does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person. It should be noted that the “weighted balance,” test, discussed in Section 2.1.4.6 above, is again used here.

2.1.5 Traffic Data and its processing

Traffic data is defined in Article 2 (1) of PECR, as “any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication.” The E-Privacy directive suggests that this definition is very broad, as recital 15 states traffic data may include any translation of information for the purpose of carrying transmitting it, data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.¹⁰⁹ There seems to be no reason why it would not be equally broad in UK law.

The processing of traffic data is regulated by s.7 of PECR, which lays down the general rule in relation to its retention, that “traffic data relating to subscribers or users which are processed and stored by a public communications provider shall, when no longer required for the purpose of the transmission of a communication, be...erased” or modified so as to no longer constitute personal data.” The ICO guidelines on this subject stress that the term ‘subscriber’ used here is wider than ‘individual,’ and that therefore data relating to corporations, which would be personal data if the corporation were an individual, are to be treated in the same way as personal data in terms of retention.¹¹⁰ However data relating to billing the subscriber may be retained until it would not be possible to sue to recover those charges, which as is stated in the ICO guidance is six years in UK contractual law.¹¹¹

More notable is the exception to the general principle: “traffic data relating to a subscriber or user may be processed and stored by a provider of a public electronic communications service if;

- such processing and storage are for the purpose of marketing electronic communications services, or for the provision of value added services to that subscriber or user; and

¹⁰⁸ Korff, 2002, 89

¹⁰⁹ Bohm, 2008, p.15

¹¹⁰ ICO, ‘ *Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003 Part 2: Security, confidentiality, traffic and location data, itemised billing, CLI and directories,*’ 2006, p. 8

¹¹¹ *ibid*



- the subscriber or user to whom the traffic data relate has given his consent to such processing or storage; and
- such processing and storage are undertaken only for the duration necessary for the purposes specified in subparagraph (a)”.

These exceptions are relatively broad as the ICO has explicitly stated there is no limit to what can constitute a ‘value added service’.¹¹² However the concept of consent is restricted here; s. 8 states that in this context consent means prior informed consent, in which the subscriber is informed about “the types of traffic data which are to be processed and the duration of such processing.” The ICO elucidates this further, explaining that the subscriber must be given sufficiently clear information for them to have a broad appreciation of how the data is going to be used and the consequences of consenting to such use.¹¹³ The ICO also states that where the value added service is provided by a third party, whoever will be seen to be responsible for providing that service should obtain the consent, as the manner in which a service is provided should be consistent with the expectations of the subscriber. Therefore when “the user provides consent to one party to provide a particular service, they should not then be surprised when they are contacted by another party relating to the provision of that service.”¹¹⁴ The ICO also gives the example of ‘catch-all’ statements put on bills, or on websites, which inform the subscriber that traffic data will be processed and assume consent in the absence of complaint; it explicitly states these systems cannot obtain valid consent in relation to s.7 of PECR.¹¹⁵ It also states subscribers must be able to withdraw consent at any time. The example of targeted advertising systems shows how broad the ambit of these provisions on traffic data is. Since even data such as what protocol the information is in is traffic data, as recital 15 of the e-privacy directive states,¹¹⁶ targeted advertising systems certainly do process traffic data. While it seems reasonable to consider targeted advertising a value added service, and so able to benefit from an exemption allowing the processing of traffic data in order to provide one of these again consent is necessary, it is difficult for them to obtain the prior informed consent, outlined above. Clearly this was not obtained in Phorm’s 2006/2007 trials, but to conform with these provisions of PECR future uses of this type of technology will need to get prior informed consent, and bearing in mind that the ICO does not seem to think general statements on bills or websites are sufficient this could pose difficulties.

2.1.6 Location Data and its processing

Location data is defined in Article 2 (1) of PECR, as “any data processed in an electronic communications network indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to...the latitude, longitude or altitude of the terminal equipment or...the direction of travel of the user or...the time the location information was recorded.” There is therefore clearly some overlap with traffic data, and in s.14 this is resolved, with it being decreed that where data qualifies as both the rules relating to traffic data shall apply.

¹¹² ibid

¹¹³ ibid, p.9

¹¹⁴ ibid,

¹¹⁵ ibid

¹¹⁶ Bohm, 2008, p.15



D7.1a User Evaluation Plan

S.14 goes on to say that “location data relating to a user or subscriber of a public electronic communications network or a public electronic communications service may only be processed... where that user or subscriber cannot be identified from such data or...where necessary for the provision of a value added service, with the consent of that user or subscriber.” Such consent must, as with traffic data, be informed, meaning that the user must be aware of the types of location data that will be processed, the purposes and duration of the processing of those data and whether or not the data will be transmitted to a third party for the purpose of providing the value added service. As with Traffic data the ICO has made it clear that placing ‘catch all’ statements on websites or bills does not constitute obtaining informed consent,¹¹⁷ and that where a value added service is provided by a third party, whoever will be seen to be responsible for providing that service should obtain the consent, as the manner in which a service is provided should be consistent with the expectations of the subscriber. S.14 of PECR not only guarantees the subscriber’s right to withdraw their confirmed consent at any time but also states that they must, “in respect of each connection to the public electronic communications network in question or each transmission of a communication, be given the opportunity to withdraw such consent, using a simple means and free of charge.” The ICO adds to this that it is possible for service providers to provide subscribers to withdraw the consent temporarily, and that where a specific length of time is specified there is nothing to stop the service provider ‘reactivating’ this consent at the end of that period without further instruction from the subscriber.¹¹⁸

Furthermore, any processing of location data can “only be carried out by - (i) the public communications provider in question (ii) the third party providing the value added service in question; or (iii) a person acting under the authority of a person falling within (i) or (ii); and (b) where the processing is carried out for the purposes of the provision of a value added service, be restricted to what is necessary for those purposes.”

Google’s Latitude project is an informative example of the application of these laws. It is a value added service under s.14 of PECR which tracks subscribers’ locations and allows them to share them with other subscribers with whom they have agreed to share.¹¹⁹ It would seem to be fully compliant with PECR as the location data of subscribers are only processed if they explicitly sign up to the service and even then it will only be tracked while they are signed into Latitude.¹²⁰ This ability to sign in and out is effectively an implementation of the ICO’s suggestion that users should be able to temporarily withdraw consent. However, Latitude, like Phorm, demonstrates the sensitivity of these issues in the UK as even though it is fully compliant with PECR, and also includes other privacy preserving mechanisms such as giving the subscriber the ability to prevent particular, or all, other users from being able to see their location, it is causing controversy. A Member of Parliament, Tom Brake, has raised the matter in parliament¹²¹ and privacy groups such as Privacy international are also

¹¹⁷ ICO, ‘Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003 Part 2: Security, confidentiality, traffic and location data, itemised billing, CLI and directories,’ 2006, p. 11

¹¹⁸ *ibid*

¹¹⁹ Google 2009

¹²⁰ *ibid*

¹²¹ Web Team, 2009



questioning the implications of this technology.¹²² Both Brake and Privacy International have drawn attention to the possibility of employers and parents giving their employees and children, respectively, phones with the technology on them so that they can be tracked, as well as the possibility that jealous partners might covertly sign their lovers up to Latitude.¹²³ To combat these problems they are suggesting that Google send daily texts alerting users that Latitude is on their phone,¹²⁴ although they don't seem to give any consideration to how annoying such a system could be.

2.1.7 Rights of the Data Subject

Bainbridge and Pearce, though not particularly impressed with the UK's implementation of the DPD in general do state that the Rights of the data subject are well protected under the DPA.¹²⁵ Before a brief outline of what they are is given it should be noted that this section should be considered in conjunction with section 2.1.4.10 which concerns the sixth data protection principle, which states that data controllers are bound to respect the rights of the data subject.¹²⁶ It should also be pointed out that under s.33 (4) data processing done for the purposes of research is exempt from s.7 of the DPA.¹²⁷

The rights of the data subject are described in Part II of the DPA. S.7 gives data subjects the right to be informed by any data controller whether personal data of which that individual is the data subject are being processed and if that is the case to be provided with a description, of the data, the purposes for which they are being processed, and the recipients to whom they are or may be disclosed. It goes on to outline the conditions under which such access is given. However, as has already been stated s.7 is of little concern to research projects. Neither is s.8 as it consists of provisions which in certain circumstances alter the workings of s.7, and nor are s.9 or s.9A which are addressed to credit reference agencies and public authorities respectively.

S.10 provides data subjects with a right to prevent processing likely to cause unwarranted substantial¹²⁸ damage or distress to the data subject or another, by notice in writing to the data controller. However this right does not exist where any of the conditions in paragraphs 1 to 4 of Schedule 2 are met,¹²⁹ or where the Secretary of State decrees otherwise by order. S.11 gives a right for individuals to require that a data controller does not begin to, or ceases within a reasonable period, processing personal data for purposes related to direct marketing, and s.12 states that by notice in writing to any data controller, a data subject can require that no decision which significantly affects them is taken based solely on processing by automatic means. The data controller is rendered liable in respect of any damage or distress caused by contraventions of the DPA by s.13 and s.14 provides for a

¹²² Privacy International, 2009

¹²³ Web Team, 2009

¹²⁴ Web Team, 2009, Privacy International, 2009

¹²⁵ Bainbridge and Pearce, 2000

¹²⁶ In fact as a research project it is probably best to look at these rights from the perspective of the sixth data protection principle, as that outlines what duties bind the data controller, rather than at the rights themselves which is a more appropriate perspective for data subjects.

¹²⁷ See also Section 2.4.4.6 above

¹²⁸ This is again the weighted balance discussed above in Section 2.4.4.2.

¹²⁹ See Section 2.4.4.1, paragraphs 3-5.



mechanism whereby a court, on the petition of the relevant data subject, can order data controllers to rectify, block, erase or destroy personal data.

2.1.8 Confidentiality of Communications

2.1.8.1 Interception

S.1 of RIPA makes the intentional interception without legal authority of any communication being transmitted by a public or private telecommunications network, or public postal service, an offence punishable by up to two years imprisonment. Interception is defined in s.2 (2), which states that “a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he, ...so modifies or interferes with the system, or its operation,...so monitors transmissions made by means of the system, or...so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication”. Notably communication is not defined although as ‘public telecommunications system,’ and ‘public telecommunications service’ are, it seems sensible to presume it means any information transferred via these.

The difficulties that arise in determining what constitutes interception are well illustrated by the example of targeted advertising systems, such as Phorm. Bohm appears to be convinced that targeted advertising technology involves the interception of communications within the meaning of s.2 (2) of RIPA, as without it becoming available to a third party, the ISP, they could not determine what a subscriber was interested in.¹³⁰ However, the Home Office in its advice to Phorm does suggest that the argument that Phorm’s processing does not constitute ‘making available’ could perhaps be viable.¹³¹ Bohm’s rebuttal of this suggestion is comprehensive; the previously dominant view that a machine cannot use information espoused by the Law Commission in 2002, has been rejected in the Serious Fraud Act 2006 and cases such as *O’Shea v. City of Coventry Magistrates Court*¹³² and even more importantly other parts of the RIPA relating to the powers given to the security services, s. 16 especially, consider even less, merely the interception a stage where it is not even decided whether the information will be examined, to be interception.¹³³

However s.2 (3) explicitly states interception does not include interception of any communication broadcast for general reception. It could perhaps be argued that websites are broadcast for general reception and so the information from them to users cannot be intercepted. However, although websites are certainly very often for ‘general reception,’ this would be in complete contradiction of the established meaning of broadcast in both common usage and under the European regulatory architecture, which defines ‘broadcast’ in Art. 1 (c) of the TVWF directive, as amended by the AVMS directive, as the provision of “simultaneous viewing of programmes on the basis of a programme schedule.” Therefore it seems that transmissions from websites to users can be ‘intercepted.’

¹³⁰ Bohm, 2008, p. 4

¹³¹ Home Office, 2008, at 9

¹³² [2004] EWHC 905

¹³³ Bohm. 2008, pp.4-5



2.1.8.2 Consent

Interception can be lawful, under s.3 (1) of RIPA, where the consent of both the sender and recipient has been obtained, or the interceptor reasonably believes that it has been. Here, unlike in the DPA, it is explicitly stated that the interceptor's reasonable belief that they had consent is sufficient, which is a considerably lesser requirement as it effectively means that for a data controller to breach s.1 of RIPA they would need to do so intentionally. Additionally, breaches of RIPA, being criminal must be proven in the context of a criminal trial, in which it would be very difficult for the prosecutor to prove beyond reasonable doubt that this was not the case. In the case of the unauthorised deployment of targeted advertising system, such as occurred in the 2006/2007 Phorm trials for example, it might be difficult to show that there was not a reasonable doubt that the ISP did reasonably believe it had consent, even if that consent were to be implied or derived from the small print of the ISP's terms of service.¹³⁴ Though there are certain categories of website about which it could be difficult to demonstrate even a reasonable doubt that perhaps the ISP thought it had consent, such as personal email accounts and online banking portals.

However it is less reasonable to assume targeted advertising systems have the consent of the other party, the website. In the HO note it is argued that perhaps the fact that websites are free for anyone to look at means that, there is an implied consent that Phorm's technology can be used to monitor who is accessing them,¹³⁵ and Phorm does appear to subscribe to this logic, as their meeting with Clayton shows.¹³⁶ This logic without justification conflates the content of the website with the information as to who is looking at it, which is in fact separate and commercially valuable data. While in the case of the user there is at least a purported benefit, more appropriate advertising, in the case of the website there clearly isn't. In fact in many cases such as Google and Amazon, the website will be in direct competition with the targeted advertising system on the advertising market, and therefore the targeted advertising system interception of the communication to glean the commercially valuable information about who visits the website, will actually be harmful to websites such as Google.¹³⁷ As targeted advertising systems know this, an assumption of consent does not seem reasonable. For targeted advertising systems to maintain that it is reasonable to assume websites publishing their content consent it must be possible to opt out of the system, or otherwise the concept of consent would be void of meaning. Here too their argument is flawed if they believe it renders their conduct legal under RIPA. It is apparently possible for websites to opt out of targeted advertising systems, though the mechanism for opting out of Phorm is somewhat unclear.¹³⁸ However this will only stop the communications from them being intercepted, not those to them, and since s.3 of RIPA requires the consent of both parties to each communication, Phorm's technology would not benefit from the exemption s.3 provides, as websites opting out would still have the communications sent to them intercepted.¹³⁹

¹³⁴ Bohm, 2008, p. 5

¹³⁵ Home Office, 2008, at 15

¹³⁶ Clayton, 2008, p.6

¹³⁷ Bohm, 2008, p.6

¹³⁸ Clayton, 2008, p. 6

¹³⁹ Bohm, 2008, p.7



It is the conception of consent used in s.3 of RIPA that is seemingly at the heart of the European Commission's infringement proceedings against the UK in relation to personal data protection.¹⁴⁰ Although RIPA predated the E-privacy directive, and its implementation in the form of PECR, the UK legislature appears to have considered it to be an effective implementation of Art 5. (1) and Art 5. (2) of the E-privacy Directive, as these provisions, which relate to the interception of communications, are not present in PECR. There is no suggestion in the E-privacy Directive that a reasonable belief on the part of the interceptor, that they have consent, can render such interceptions lawful. However, RIPA does allow this far less stringent requirement in relation to consent to render interceptions lawful, and that appears to be what the Commission is concerned about.¹⁴¹ Especially as it may mean that Phorm's secret 2006/2007 trials do not breach UK 'interception of communications' laws.¹⁴² Certainly at least one UK police force¹⁴³ considers that implied consent was present the 2006/2007 trials, and this fact has contributed to the European Commission's resolve to bring infringement proceedings against the UK in relation to these matters.¹⁴⁴

2.1.8.3 Connected services

Under s.3 (3) of RIPA if the interception is conducted "by or on behalf of a person who provides a ...telecommunications service; and...it takes place for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services." This exemption is perhaps a better justification for interceptions such as those performed by targeted advertising services, but whether it is valid obviously hinges on the interpretation given to the phrase "for purposes connected to." The phrase itself gives no indication as to what degree of connection is required, and as it is only the phrase that is legally binding the following is mere conjecture. Bohm draws attention to the close connection present in the example of an interception that would benefit of the exemption under s.3 (3) given in the explanatory notes to the RIPA; "where the postal provider needs to open a postal item to determine the address of the sender because the recipient's address is unknown," as well as the close connection in interceptions accepted as falling within this exemption such as filtering out junk mail.¹⁴⁵ However, this is not conclusive evidence that activities that are less closely associated would not qualify. Bohm also argues persuasively, in the context of Phorm, that the commercial reality is that interceptions by services such as targeted advertising systems are more closely connected to the services provided by the targeted advertising systems than those provided by the ISP, since the revenue stream from using the technology belongs to the targeted advertising system rather than the ISP, or at least it does in the case of Phorm.¹⁴⁶ However there is nothing in the act to say that interception cannot be connected to more than one service.

¹⁴⁰ Europa Press Releases Rapid, 2009

¹⁴¹ Europa Press Releases Rapid, 2009

¹⁴² *ibid*

¹⁴³ The UK police are divided into regional constabularies, or 'forces,' which deal with criminal complaints, such as those concerning RIPA, independently (UK Police Portal Team, 2009).

¹⁴⁴ European Commission, "Progress Report on the Single European Electronic Communications Market 2008 (14th Report)," 2009, p. 346

¹⁴⁵ The Crown, 2000, at 40

¹⁴⁶ Bohm, 2008, p.10



2.1.8.4 Accessing and storing information on users' terminal equipment

This is the only aspect of Art. 5, 'Confidentiality of the Communications,' of the E-privacy Directive that has been implemented through PECR, the first two subparagraphs being dealt with under the RIPA. This section could perhaps alternatively be titled 'cookies,' as that is largely what it is concerned with, that and the prohibition of spyware and its ilk.¹⁴⁷ It is also important to note that this section may provide additional protection to that derived from the DPA as it is not limited in its scope to personal data.

S.6 of PECR states that "subject to paragraph (4), a person shall not use an electronic communications network to store information, or to gain access to information stored, in the terminal equipment of a subscriber or user unless [the] subscriber or user of that terminal equipment is (a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and (b) is given the opportunity to refuse the storage of or access to that information." It also states that consent need not be sought for every act that would otherwise breach s.6, but that an initial consent is sufficient. This type of consent is obviously more stringent than that required by RIPA and more akin to that elsewhere in PECR in relation to traffic and location data. Furthermore, the ICO has stated that the 'opportunity to refuse' constitutes more than merely the possibility of refusal, but that rather a mechanism by which a subscriber can refuse continued storage must "be prominent, intelligible and readily available to all, [and] not just the most computer literate or technically aware."¹⁴⁸ Where cookies come from a third party, meaning a party other than the primary website the user is viewing, as may be the case with third party advertising, the ICO states that both the primary website and the third party will be responsible for obtaining consent.¹⁴⁹ It further states that as regards the primary website a statement stating that it cannot be held responsible for the use of cookies by third parties will not be sufficient.¹⁵⁰

Paragraph (4) states that the prohibitions of s.6 do not apply in the case of "the technical storage of, or access to, information (a) for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network" or interestingly "where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user." The ICO states that 'strictly necessary,' "means that such storage of or access to information should be essential, rather than reasonably necessary."¹⁵¹

Targeted advertising systems certainly seem to come within the ambit of the 'covert surveillance mechanisms' with which the ICO states this provision is concerned,¹⁵² but they can perhaps be

¹⁴⁷ ICO, 'Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003 Part 2: Security, confidentiality, traffic and location data, itemised billing, CLI and directories,' 2006, p. 4

¹⁴⁸ On p. 5 of *ibid*, the ICO recommends referring to the Interactive Advertising Bureau advice concerning cookies available at www.allaboutcookies.org, in order to make sure that websites use a mechanism that obtains consent compatible with s.6 of PECR.

¹⁴⁹ *ibid*, p. 6

¹⁵⁰ *ibid*, p. 6

¹⁵¹ *ibid*, p. 6

¹⁵² *ibid*, p. 4



rendered legitimate, by the presence of suitable consent. However, the ICO appear to have indicated that BT breached PECR by deploying Phorm in the 2006/2007 trials without consent.¹⁵³

2.1.9 Direct Marketing¹⁵⁴

Direct marketing is defined in s.11 (3) of the DPA as “the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.” The ICO promotes a broad conception of this definition, which covers the promotion of an organisation’s aims and ideals as well as offerings of goods or services. The UK Information Tribunal supported this approach ruling that automated calls from the Scottish National Party canvassing for support were direct marketing.¹⁵⁵

The substance of s.11 of the DPA is that “at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing for the purposes of direct marketing personal data in respect of which he is the data subject.” It goes on to give courts the power to order compliance with this rule.

This is also further regulated under PECR. S.19 makes it a breach of PECR to make unsolicited automated phone calls without prior permission, while s.21 states that if they are not automated there must merely be the possibility for the recipients to opt out, both directly in relation to that particular caller and generally through putting themselves on the Telephone Preference Service (TPS) register. It is only permissible, under s.22, to send unsolicited marketing material by electronic mail, which according to the ICO includes email, text and picture messaging,¹⁵⁶ with the consent of the addressee. The ICO has stated that this rule is intended to be technologically neutral and so cover new mechanisms that arise for sending messages as well.¹⁵⁷ Consent here, according to the ICO means “individuals must fully appreciate that they are consenting and must fully appreciate what they are consenting to.”¹⁵⁸ However the ICO concedes that there are various mechanisms through which such consent can be obtained, some of which are strictly opt-out mechanisms, such as systems where a prominent message is displayed informing the user about what they are consenting to if they do not tick an ‘opt-out’ box.¹⁵⁹ There is also another exception to s.22; it is permitted to send unsolicited marketing material by electronic mail where the individual's details were obtained in the context of a commercial relationship and the marketing relates to similar products or services. Further, s.23 dictates that unsolicited electronic mail is entirely prohibited where it either conceals the sender’s identity, or

¹⁵³ Paladine, 2008

¹⁵⁴ The ICO’s guidance in relation to direct marketing is detailed and practical., and available online: Information Commissioner’s Office, ‘*Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003*,’ 8th October 2008, online at http://www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/guidance_part_1_for_marketers_v3.1_081007.pdf, last checked 24/08/2009

¹⁵⁵ ICO, ‘*Scottish National Party (SNP) found in breach of privacy regulations*,’ 2006, p. 1

¹⁵⁶ ICO, ‘*Your legal obligations*,’ 2009. The ICO has stated that the regulations in PECR

¹⁵⁷ ICO, 2008, p. 3

¹⁵⁸ *ibid*, p.6

¹⁵⁹ *ibid*, p. 5



does not give an address to which a request that such e-mails cease can be sent. It also regulates unsolicited messages sent by fax.

The rules derived from PECR will apply to any direct marketing exercise, but s.11 of the DPA, and in fact all the other rules in the DPA, will only apply to the exercise if it involves the processing of personal data. The ICO's guidance helpfully states that while a list of phone numbers does not, a list of phone numbers with accompanying names normally would.¹⁶⁰

2.1.10 Data Retention

Where the data being retained is personal data the data protection principles will apply. How long a data controller may retain data is dealt with under the third and fifth principles.¹⁶¹ Furthermore whether the data is personal or not if it constitutes traffic data its retention will be governed by s.7 of PECR which is discussed above in Section 2.1.5 'Traffic data and its processing'.¹⁶²

The Data Retention Directive,¹⁶³ has been implemented into UK law in the form of the Data Retention (EC Directive) Regulations 2009 (DRR).¹⁶⁴ However the legality of the directive is open to some debate, which is briefly examined below in section 2.2.10 'Data Retention.' It concerns the treatment of 'communications data,' which according to s.2 (b), "means traffic data and location data and the related data necessary to identify the subscriber or user." The last element of this definition appears to suggest that any set of communications data relating to an individual will also be personal data, as it can identify the individual. Only 'public communications providers' are subject to the DRR. They are, according to s.2 (e) of the DRR, either providers of a public electronic communications network, or providers of a public electronic communications service.¹⁶⁵

S.4 of the DRR obliges public communications providers to retain the communications data specified in the schedule to the Regulations. In relation to fixed and mobile telephony this includes the calling and receiving telephone numbers, the names and addresses of the subscribers or registered users of the

¹⁶⁰ ICO, 2008, pp. 3-4

¹⁶¹ See Sections 2.44.3 and 2.4.4.5 above for a more detailed analysis of the obligations imposed by these principles.

¹⁶² second paragraph

¹⁶³ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal L 105*, 13/04/2006 P. 0054 – 0063, online at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML>, last checked 24/08/2009

¹⁶⁴ Statutory Instrument 2009, Number 859, 2nd April 2009, online at http://www.opsi.gov.uk/si/si2009/plain/uksi_20090859_en_1, last checked 24/08/2009

¹⁶⁵ 'Public electronic communications network' and 'public electronic communications service' have the meaning given in section 151 of the Communications Act 2003 (c. 21), 'An Act to confer functions on the Office of Communications; to make provision about the regulation of the provision of electronic communications networks and services and of the use of the electro-magnetic spectrum; to make provision about the regulation of broadcasting and of the provision of television and radio services; to make provision about mergers involving newspaper and other media enterprises and, in that connection, to amend the Enterprise Act 2002; and for connected purposes,' 2003, online at http://www.opsi.gov.uk/ACTS/acts2003/ukpga_20030021_en_1, last checked 24/08/2009



aforementioned numbers, the date and time of the start and end of the call and the telephone service used. In relation to mobile telephony this additional information must also be retained; the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI) of the telephone calling and receiving telephones, the cell ID at the start of the communication, data identifying the geographic location of cells by reference to their cell ID, and if it is a pre-paid anonymous service, the date and time of the initial activation of the service and the cell ID from which the service was activated. In relation to internet access, internet e-mail or internet telephony, the following must be retained; the user ID allocated, the user ID and telephone number allocated to the communication entering the public telephone network, the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication, the date and time of the log-in to and log-off from the internet access service, the IP address, the user ID of the subscriber or registered user of the internet access service, in the case of dial-up access, the calling telephone number or in other cases, the digital subscriber line (DSL) or other end point of the originator of the communication. In the case of internet telephony, the user ID or telephone number, and the name and address of the subscriber of the intended recipient of the call must also be retained. In the case of e-mails, the name or registered user and the user ID of the intended recipient of the communication, and the date time and duration of the login to the e-mail service must be held.

This information, according to s.5 must be retained for 12 months, and s.7 states that the data can only be accessed in specific cases and in accordance with the law.

The retention of data in order to fulfil obligations imposed by the data retention directive is presumably neither excessive under the Second Principle nor unnecessary under the Fifth Principle, since it is statutorily justified. The ICO has specifically stated that the provisions of other legislative acts specifically affect the meaning of necessary in the Fifth Principle.¹⁶⁶ Reconciling the provisions of s.7 of PECR and the DRR is more difficult as while the former states traffic data should be erased once it no longer needed for transmission the latter states it should be retained for twelve months. It seems the only suitable solution is the UK doctrine of ‘implied repeal’ whereby the more recent law is superior to the older one. This would result in the traffic data being held for 12 months before being destroyed in accordance with s.6 (1)(d) of the DRR: “except in the case of data lawfully accessed and preserved, the data retained solely in accordance with these Regulations must be destroyed at the end of the retention period.”

2.1.11 Other Relevant Laws

2.1.11.1 Fraud

S.2 of the Fraud Act 2006 (c. 35)¹⁶⁷ makes it an offence to dishonestly make a false representation, with the intention of making a gain for himself or another. It goes on to state “a representation is false if...it is untrue or misleading, and...the person making it knows that it is, or might be, untrue or

¹⁶⁶ ICO, 2001, p. 39

¹⁶⁷ ‘An Act to make provision for, and in connection with, criminal liability for fraud and obtaining services dishonestly,’ 8th November 2006, online at http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060035_en.pdf, last checked 11/07/2009



misleading,” “that a representation may be express or implied,” and most vitally that a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).”

The core of targeted advertising technologies such as Phorm cannot help falling foul of this provision, as it involves a machine imitating the website requested by the user, in order to place the cookie containing the UID on the user’s machine, which, especially bearing in mind the explicit reference to a representation being made where information is submitted to a communications device, clearly constitutes the making of a false representation.¹⁶⁸ The criterion that the false representation is made in order to make a gain, is almost certainly fulfilled where the repeated making of it is the lynchpin of a technology that forms the main asset of a listed company, as it does in the case of Phorm. However, whether or not the representation is dishonest is obviously a matter to be decided by a jury, but Bohm sensibly holds that where the representation is made where there is intentionally no chance for the owner of the device to consent to it being made, or where it is made in the context of what he calls Phorm’s “exaggerated claims [of] anonymity,” the grounds for finding dishonesty would be strong.

2.1.11.2 Trademark Infringement/Passing Off

The implications of this area of law will not be explored in detail as they are very complex and relatively distant from the immediate subject of data protection and privacy. It will be sufficient to note, that the use of other websites names in cookies in the rigmarole involved in planting the UID containing cookie on the users system could be considered to be the ISP passing itself off as the website concerned. This might well be defamatory if the website concerned states anywhere specifically that it respects its users’ privacy or does not monitor their behaviour.¹⁶⁹

2.1.11.3 Trespass to goods

The Tort (Interference with Goods) Act 1977 (c.32)¹⁷⁰ iterates the common law principle that “wrongful interference with goods” is an actionable tort. This is clearly a very vague rule that can only function as law because it exists in the context of hundreds of years of case law. None of that case law yet relates to a party detrimentally and without their permission affecting the performance of their computer. However, there is an American case from the United States District Court for the Northern District of California, *Ebay Inc. v. Bidder’s Edge, Inc*¹⁷¹ in which it was held that visiting a competitors website so much it reduced its performance was a tort. This could have implications for technology such as Phorm, which obviously through the sending of extra requests to machines in order to place a cookie slows them down. However, this area of law has not yet developed in the UK to include this ‘cyber-trespass.’¹⁷²

¹⁶⁸ Bohm, 2008, p. 12

¹⁶⁹ Bohm, 2008, p.16

¹⁷⁰ ‘An Act to amend the law concerning conversion and other torts affecting goods,’ 22nd July 1977, online at http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1977/plain/cukpga_19770032_en, last checked 11/07/2009

¹⁷¹ No C-99-21200 RMW

¹⁷² Hanff, 2008, p. 17



2.1.12 Conclusion

The obligations imposed by the data protection laws and authorities in the UK are not amongst the most stringent in Europe. Some, like Pounder, even go as far as to say that UK governments regulate these matters in such a way as to intentionally limit the effects of directives relating to privacy.¹⁷³

However, as examples such as Phorm and Latitude show, that does not mean a lax approach to data protection, which Korff maintains is endemic in Europe,¹⁷⁴ can be justified in the UK as the public awareness and concern about these issues is significant, especially in the context of electronic communications. In being stringently compliant with data protection laws in the UK the resources made available by the ICO are extremely helpful, particularly the guidance it gives on how to perform a Privacy Impact Assessment.¹⁷⁵

¹⁷³ 'Europe claims UK botched one third of Data Protection Directive,' 2007

¹⁷⁴ Korff, 2002, p. 239

¹⁷⁵ Information Commissioner's Office, 'Appendix 1 PIA screening process,' 2009, online at http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/3-app1.html, last checked 24/08/2009



2.2 Germany

2.2.1 Introduction

Issues of data protection, as well as other issues relating to human rights, have been afforded special importance in Germany since the Second World War, as Chapter 1 of the Basic Law for the German Republic, the *Grundgesetz für die Bundesrepublik Deutschland* (GG),¹⁷⁶ makes clear.¹⁷⁷ S.10 of the GG addresses explicitly the confidentiality of communications, and since the groundbreaking 1983 *Census Case*,¹⁷⁸ it has been held that a right to privacy can be derived from s.2 (1), the general right to respect for one's personality, *das allgemeine Persönlichkeitsrecht*,¹⁷⁹ read in conjunction with Art.1 (1), which concerns human dignity generally. It also appears that the extensive surveillance carried out by the *Ministerium für Staatssicherheit*, the Stasi, in the German Democratic Republic, has increased further the public awareness and political importance of data protection issues in Germany.¹⁸⁰

It was therefore not the DPD that first created the necessary momentum to legislate in relation to matters of data protection, as it did in many other European countries. The first *Land* to adopt a data protection law, Hesse, did so in 1970, and the Federal Data Protection Act, the *Bundesdatenschutzgesetz* (BDSG),¹⁸¹ which states boldly that its purpose is to “protect the individual against his right to privacy being impaired through the handling of his personal data,”¹⁸² was passed in 1977. This has since been modified, most notably in 2001 in order to ensure Germany was entirely compliant with the DPD.¹⁸³

S.1 (2) of the BDSG states that the BDSG applies to the collection, processing and use of data by both private bodies and federal public bodies, though to the public bodies of the 16 Lander in only very

¹⁷⁶ 23th May 1949 (Federal Law Gazette I, No. 1 of 23.05.1949, p. 1). An English translation has been made available online by The Comparative Law Society at: <http://www.iuscomp.org/gla/statutes/GG.htm#10>. All extracts in this text that purport to be from the GG have been taken from this text, which includes amendments up to and including those of 20th December 1993.

¹⁷⁷ It contains a list of basic human rights which “bind the legislature, the executive, and the judiciary as directly applicable law,” and in s.1 it is acknowledged that “inviolable and inalienable human rights [are] the basis of every community of peace and of justice in the world.”

¹⁷⁸ 15. December 1983 (AZ. 1 BvR 209, 269, 362, 420, 440, 484/83)

¹⁷⁹ Korff, 2002, p.14

¹⁸⁰ Current issues of data protection are still often discussed in the context of the Stasi's surveillance regime, as *Der Spiegel's* coverage of Lidl's monitoring of its employees (Lill, 2008), and Forbes' coverage of Deutsche Bank's behaviour (Ram, 2009), amongst others, demonstrates.

¹⁸¹ 27th January 1977 (Federal Law Gazette I No. 7 of 01.02.1977, p. 201). An English translation has been made available by the BfDI online at: <http://www.bfdi.bund.de/cae/servlet/contentblob/411288/publicationFile/25384/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf>. All extracts in this text that purport to be from the BDSG have been taken from this text which includes amendments up to and including those of 15 November 2006.

¹⁸² S.1 (1) of the BDSG

¹⁸³ Born, 2001



D7.1a User Evaluation Plan

limited circumstances.¹⁸⁴ Data processing, collection and use by public bodies is addressed in Part II of the BDSG, while processing, collection and use by private parties is dealt with in Part III. This report will concentrate on the latter as the PICOS project is a private body, and the important distinction between public and private bodies will be elucidated below in section 2.2.4.3 'The distinction between public and private bodies.'

The rules contained in the BDSG act as a 'safety net,' or 'cushioning legislation,'¹⁸⁵ only applying, according to s.1 (3), in circumstances in which there are not more specific federal legal provisions governing data protection.¹⁸⁶ Therefore more specific statutes will generally apply in place of the BDSG though where the Telecommunications Act does not deal with a case conclusively, the BDSG will supplement it.¹⁸⁷ The most significant of these in the area of electronic communications is the Telecommunications Act, the *Telekommunikationsgesetz* (TKG)¹⁸⁸ which was significantly modified in June 2004 in order to incorporate provisions implementing the E-privacy directive.

It should also be stated that, as in most EU Member States,¹⁸⁹ none of the German data protection laws contain provisions mirroring Art. 3(2) of the DPD or Art. 1(3) of the E-Privacy Directive, which limit their scope to that of the Treaty establishing the European Community, therefore excluding topics such as those covered by Titles V and VI of the Treaty on European Union.

Each of the 16 Lander also regulates data protection at state level, though the focus of this report will be the Federal legislation as to examine each of the Data Protection Acts of the 16 German *Länder* in detail would be beyond the scope of this report.

It is important to note that over the last few years Germany has been host to a considerable number of scandals related to data protection. A number of them involved the monitoring of employees by employers, for example Lidl was found to be secretly filming staff and keeping detailed records of their behaviour,¹⁹⁰ Deutsche Bahn was discovered to have hired private investigators to monitor its staff¹⁹¹ and it was revealed that Deutsche Telekom had monitored the phone calls of their executives.¹⁹² Deutsche Bank has also been accused of breaking data protection laws in their treatment

¹⁸⁴ Where data protection is not governed by *Land* legislation and in so far as the body executes federal law or acts as body of the judicature not dealing with administrative matters.

¹⁸⁵ Born, 2001

¹⁸⁶ S.1 (4) of the BDSG adds that legal obligations to maintain secrecy or professional or special official confidentiality shall still be binding, even if they are not based on legal provisions in either the BDSG or more specific legislation.

¹⁸⁷ Working Party 11, 2007, p. 79

¹⁸⁸ 25th July 1996 (Federal Law Gazette I, No. 39, 31.07.1996, p. 1120). An English translation has been made available by the BfDI online at:

<http://www.bfdi.bund.de/cae/servlet/contentblob/411286/publicationFile/25386/TelecommunicationsAct-TKG.pdf>, All extracts in this text that purport to be from the TKG have been taken from this text, which includes amendments up to and including those of the 22nd June 2004. However it has since been further amended, most recently on the 21st December 2007 (No. 70, 31.12.2007, p. 3198), and the provisions resulting from these amendments will be duly included in this report as well.

¹⁸⁹ Korff, 2004, p.41

¹⁹⁰ Lill, 2008

¹⁹¹ Moore, 2009

¹⁹² Jtw, 2009



of their employees.¹⁹³ Other problems have arisen in relation to the buying and selling of personal data. A whistleblower working in a call centre in Schleswig-Holstein informed the *Land's* data protection commissioner of the misuse of personal data at his place of work, giving them a sample of 17,000, from a claimed total of 1.5 million, sets of personal data, including individuals' addresses and bank account details.¹⁹⁴ A federation of German consumer organisations also demonstrated that it was possible to quite easily buy large amounts of such data for relatively small sums¹⁹⁵ and Deutsche Telekom became embroiled in these particular scandals, when it was revealed that some of the data being sold originated from their databases.¹⁹⁶ These incidents and others led to suggestions that the market in illicit personal data in Germany was much larger.¹⁹⁷

This raft of well publicised recent breaches of data protection laws, and the uproar they generated, led to the passing of a 'Law amending Data Protection Regulations' (*Gesetz zur Änderung datenschutzrechtlicher Vorschriften*¹⁹⁸) in August this year. The reforms it has introduced will be described in the relevant sections, and although it is not yet possible to judge their effectiveness, whether in the words of the *Datonomy* they will be a tiger or a paper tiger,¹⁹⁹ the European Commission does appear to be satisfied with them.²⁰⁰ It is also important to note that the vast majority of changes resulting from this reform have already come into effect, on the 1st September 2009.²⁰¹ Where this is not the case it will be stated.

2.2.2 Regulatory bodies and their powers

2.2.2.1 Federal Data Protection Commissioner (BfDI)

The Federal Commissioner for Data Protection and Freedom of Information, *der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (BfDI), and his powers, were created by the BDSG, in Part II Chapter III, specifically in s.22 and 23.²⁰² The BfDI is a public law official who is "independent in the performance of his duties and subject to the law only,"²⁰³ though he is subject to the legal supervision of the Federal Minister for the Interior. The BfDI is also based in the Federal Ministry of the Interior,²⁰⁴ and relies on it to provide him with the necessary personnel and resources to

¹⁹³ Ram, 2009

¹⁹⁴ De Quetteville, 2008

¹⁹⁵ De Quetteville, 2008. The bank details of more than 4 million people were apparently bought for £500 (.

¹⁹⁶ DW staff, 2008

¹⁹⁷ DW staff, 2008

¹⁹⁸ 14th August 2009 (Federal Law Gazette I, No. 54, 19.08.2009, p. 2814).

¹⁹⁹ Kbs, 2009

²⁰⁰ European Commission, "Progress Report on the Single European Electronic Communications Market 2008 (14th Report)," 2009, p. 117.

²⁰¹ Schweinoch, 2009, p. 6

²⁰² The BfDI's powers have since been extended to also cover the monitoring of compliance with the Freedom of Information Act, the Informationsfreiheitsgesetz (IFG), passed on the 5th September 2005 (Federal Law Gazette I, No. 57, 13.09.2005, p. 2722) which gives citizens a right to access information held by the federal authorities. The current BfDI is Peter Schaar (BfDI, '*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, stellt sich vor,*' 2009).

²⁰³ S.22 (4) of the BDSG

²⁰⁴ BfDI, *Aufgaben*, 2009



perform his task.²⁰⁵ His office is divided into eight specialised departments,²⁰⁶ the most relevant of which, for the purposes of this report, is Unit VIII which is concerned with telecommunications and media services.²⁰⁷

S. 24 of the BDSG states that the task of the BfDI is to monitor compliance with the provisions of the BDSG and other data protection provisions by public bodies of the Federation, including in relation to personal data obtained by public bodies of the Federation on the contents of and the specific circumstances relating to correspondence, postal communications and telecommunications and personal data subject to professional or special official secrecy.

Although in terms of the powers granted to it under the BDSG the BfDI has little relevance to data processing, collection and use by private bodies, under the s.115 (4) of the TKG it is given the additional responsibility of monitoring compliance with data protection legislation “as far as the data of natural or legal persons are collected, processed or used for the commercial provision of telecommunications services...as provided for by sections 21 and 24 to 26(1) to (4)” of the BDSG.” Telecommunications services are “services normally provided for remuneration consisting in, or having as their principal feature, the conveyance of signals by means of telecommunications networks, and includes transmission services in networks used for broadcasting.”²⁰⁸ These provisions give anyone the right to appeal to the BfDI if they believe that their rights have been infringed through the collection, processing or use of their personal data,²⁰⁹ and oblige telecommunications providers to assist the BfDI and his assistants in the performance of their duties by providing information in reply to their questions as well as the opportunity to inspect all documents, especially stored data and data processing programs, and to grant access to their premises at any time.²¹⁰ Where the BfDI discovers that data protection laws are being infringed, he must lodge a complaint with the appropriate regulatory authority, which in the case of telecommunications operators is BnetzA, described below in section 2.2.2.2,²¹¹ and request from that authority a statement that describes the measures taken as a result of the Federal Commissioner’s complaint.²¹² Although under s.25 (2) the BfDI can dispense with complaints itself, ‘especially if the irregularities involved are insignificant or have meanwhile been rectified.’ Furthermore, as well as informing the Regulatory Authority, under s.24(5) the BfDI is also obliged to inform the subject of its monitoring or about what it has discovered and may also submit proposals for improving its data protection.

Under s.26 of the BDSG the very important advisory role of the BfDI is outlined, whereby it must submit an activity report to the parliament every two years, must respond to requests for advice by the parliament and federal government, cooperate with other supervisory authorities dealing with data

²⁰⁵ S.22 (5) of the BDSG

²⁰⁶ BfDI, *Aufgaben*, 2009

²⁰⁷ BfDI, *Referat VIII*, 2009

²⁰⁸ S.3 No. 24 TKG

²⁰⁹ S.21 BDSG

²¹⁰ S.24 (4) BDSG

²¹¹ This is decreed in s.115 (4) of the TKG, which supplements the provisions for complaint making found in s.25 of the BDSG. The BfDI is also obliged to transmit to the Regulatory Authority any results of further monitoring after the complaint has been made (s.115 TKG (4)).

²¹² S.25 (1) and (3) BDSG



protection and may of its own accord make recommendations for the improvement of data protection in Germany.

The BfDI also maintains a registrar of data controllers indulging in automated processing, including telecommunications providers.²¹³

2.2.2.2 Regulatory Authority for Telecommunications and Posts (BnetzA)

The Regulatory Authority for Telecommunications and Posts, the *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, kurz Bundesnetzagentur* (BnetzA) is a higher federal authority responsible to the Federal Ministry of Economics and Labour.²¹⁴ It is the regulatory authority responsible for giving orders and taking other measures to secure compliance with the data protection provisions found in the TKG.²¹⁵ In order to secure such compliance it has the power to oblige communications providers to provide it with information and to enter and inspect, during normal business or working hours, business premises and production sites.²¹⁶ The extent of its considerable powers are detailed in s.127-129, and include the power to seize, subject to the granting of a court order by the local court,²¹⁷ information, including even information on their economic situation,²¹⁸ and objects,²¹⁹ where providers neglect their obligation to hand it over voluntarily.

The measures that BnetzA is authorised to take where it finds an operator is breaching the provisions of the TKG are detailed in s.126 of the TKG. It must request that the undertaking concerned state its views and take action to remedy its compliance problems,²²⁰ and where such remedial actions are not taken within the reasonable time limit set by BnetzA it may take such measures as are necessary to secure adherence,²²¹ which include a penalty of up to €500,000.²²² However, in s.149 it is stated that the fines for a number of specific breaches of the TKG relating to data protection may not exceed lesser amounts.²²³ Additionally, in the case of serious or repeated breaches of obligations by the undertaking, or failure to comply with orders issued by BnetzA demanding remedial action, BnetzA may prohibit wholly or partially the undertaking acting in the capacity of telecommunications network operator or service provider, if less severe action is insufficient.²²⁴ These potent enforcement powers make BnetzA a strong regulator, as least relatively to those in other member states.

²¹³ This is apparent from s.4e of the BDSG which requires that such processors notify them they are automatically processing personal data.

²¹⁴ S.116 TKG

²¹⁵ S.115 (1) TKG

²¹⁶ S.115 (1) TKG

²¹⁷ S.127 (6) TKG

²¹⁸ S.127 (2) TKG

²¹⁹ S.129 TKG

²²⁰ S.126 (1) TKG

²²¹ S.126 (2) TKG

²²² S.126 (5) TKG

²²³ Fines for breaches of s. 90 (3), advertising transmitting equipment, may not exceed €100,000, and for breaches of s.95(2) or s.96(2) or (3), using data, or s.96(2), s.97(3), or s.106(2), failing to erase data or documents, may not exceed €300,000.

²²⁴ S.115 (3) TKG and s.126 (3). Under s.126 (4) BnetzA, may deviate from the procedure outlined and issue provisional measures where, undertakings breaches of obligations represent either a direct and serious threat to



2.2.2.3 The Data Protection Commissioners of the Länder

Data processing, collection and use by private bodies other than telecommunications operators and service providers is monitored by the Data Protection Commissioners of the *Länder*, whose existence is justified by s.38 of the BDSG. Where such authorities discover breaches of data protection legislation they may notify the affected data subjects and the authorities responsible for prosecution or punishment.²²⁵ Where the breach is serious they may also notify the trade supervisory authority in order to initiate measures under industrial law.²²⁶ As in the case of the BfDI, anyone has the right to appeal to the Data Protection Commissioners of the *Länder* if they believe that their rights have been infringed through the collection, processing or use of their personal data,²²⁷ those being monitored are obliged to provide it with all the information necessary for the performance of its duties,²²⁸ it may enter their premises in order to investigate the standard of data protection present,²²⁹ and may impose fines in response to breaches discovered.²³⁰ These fines may be imposed whenever an administrative offence has been committed either negligently or intentionally.²³¹ Administrative offences, a full list of which can be found in s.43 of the BDSG, include failing to submit a notification or appoint a DPO when obliged to, and collecting, retrieving or processing personal data without authorisation. These offences are punishable by a maximum fine of €50,000 in the case of less serious offences like failing to notify appropriately, and €300,000 in the case of more serious offences like reversing the anonymisation process so as to reidentify individuals or unauthorised data processing, collection or use.²³² The recent reforms have also made it possible to exceed these limits if the financial benefit gained by the offender as a result of the administrative offence was higher than the maximum fine.²³³ These fines, though imposed administratively, can be appealed judicially.²³⁴

The Data Protection Commissioners of the *Länder* are also authorised, by s.38 (5) of the BDSG to require that specific technical or organisational measures must be taken to rectify irregularities discovered. Furthermore, in the event of serious irregularities it may prohibit the use of particular procedures if the irregularities are not rectified within a reasonable period contrary despite the imposition of a fine.²³⁵

The Data Protection Commissioners of the *Länder* are also obliged to keep a public register of the automated processing operations which are subject to obligatory registration in accordance with s.4d

public safety or will create serious economic or operational problems for other providers or users of telecommunications networks or services.

²²⁵ S.38 (1) BDSG

²²⁶ S.38 (1) BDSG

²²⁷ S.38 (1) BDSG

²²⁸ S.38 (3) BDSG

²²⁹ S.38 (4) BDSG

²³⁰ S.38 (5) BDSG

²³¹ S.43 (1) BDSG

²³² Schweinoch, 2009, p. 5. In terms of the BDSG these fines are outlined in S.43 (3), as modified this year. It should be noted that the processes by which fines may be imposed, and their size, do vary to some degree between the *Länder*.

²³³ Schweinoch, 2009, p. 5

²³⁴ Beyleveld et al, 2004, p. 137

²³⁵ S.38 (5) BDSG



of the BDSG.²³⁶ This register must be open to inspection by any person though the right to inspection does not extend to the general description enabling preliminary assessment as to whether the measures to guarantee the safety of processing are adequate.²³⁷

It is also for the Data Protection Commissioners of the *Länder* examine the compatibility of draft rules of conduct regarding data protection submitted by professional associations and other associations in accordance with s.38a of the BDSG. Such rules of conduct do exist in relation to scientific research, and those working for projects such as PICOS should observe them. However as Oellers and Wegner conclude, the general rules of conduct for scientists in Germany²³⁸ are almost entirely concerned with how scientists and researchers should treat one another, rather than how they should treat data subjects.²³⁹ The rules of conduct for sociologists²⁴⁰ are far more useful in this respect, going into some detail about how data subjects should be treated; the rules of conduct for example state that data subjects should only be involved in research with their informed consent, meaning that they are fully aware of any risks involved.

2.2.2.4 Public Prosecution Offices of the Länder

Every Regional Court in Germany has an accompanying Public Prosecution Office, resulting in their being a total of 116, which are subordinate to their respective Regional Public Prosecution Offices, which are established at each of the 25 Higher Regional Courts. The Regional Offices are subordinate to the Ministers of Justice of their *Länder*.²⁴¹ These Offices are responsible for investigating and prosecuting criminal offences in Germany,²⁴² most relevant of which to this report are the penal provisions found in s.148 of the TKG discussed below under section 2.1.8 ‘Confidentiality of Communications,’ and the criminal offences found in Part V of the BDSG. These offences make it a criminal offence, punishable by up to two years in prison,²⁴³ to commit any of the administrative offences in s.43, described above in section 2.2.2.3 ‘The Data Protection Commissioners of the *Länder*,’ for payment or with the intention of enriching himself or another person or with the intention of harming another person.²⁴⁴ However no one may be prosecuted under s.44 *ex officio*; a complaint must be filed with the prosecutor by the data subject, the BfDI, or a *Land* Data Protection Commissioner.²⁴⁵

The Public Prosecution Offices of the *Länder* appear to be relatively active in their pursuit of those criminally breaching data protection laws. For example, Bonn’s²⁴⁶ Public Prosecution Office is currently investigating Deutsche Telekom in relation to its monitoring of journalists and its

²³⁶ S.38 (2) BDSG. This is discussed in more detail below in section 3.4.3, ‘Data Controllers’ duties.’

²³⁷ S.38 (2) BDSG. This is discussed in more detail below in section 3.4.3, ‘Data Controllers’ duties.’

²³⁸ Deutsch Forschungsgemeinschaft, 1998

²³⁹ Oellers and Wegner, 2009, p.4

²⁴⁰ Deutsch Gesellschaft für Soziologie, ‘*Ethik-Kodex*,’

²⁴¹ Siegismund, 2003, p. 60.

²⁴² Siegismund, 2003, p. 60.

²⁴³ Imprisonment is a very unlikely consequence of data protection breaches though (Beyleveld et al, 2004, p. 137).

²⁴⁴ S.44 BDSG

²⁴⁵ S.44 (2) BDSG

²⁴⁶ Bartsch et al, 2008



supervisory board, Berlin's, Munich's and Cologne's Public Prosecution Offices are investigating thefts of personal data from Deutsch Telekom, and Bremen's Public Prosecution Office is investigating the unauthorised accessing of personal data at Deutsch Telekom.²⁴⁷ Berlin's Public Prosecution Office has also been investigating accusations of wrongdoing at Deutsch Bahn.²⁴⁸

2.2.3 Personal Data

2.2.3.1 Definition

In s.3(1) of the BDSG personal data is defined as “any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject),” and unlike in the UK this definition has been left by the courts to retain its natural meaning.

It is also important to note that in the context of the TKG the concept of ‘customer data,’ which means “the data of a subscriber collected for the purpose of establishing, framing the contents of, modifying or terminating a contract for telecommunications services,”²⁴⁹ is also important. It is difficult to imagine a scenario when this data will not also constitute personal data as it will invariably include at least the name and address of subscriber, the subscribers banking information and details concerning the service the contract is for.²⁵⁰

2.2.3.2 Special categories of personal data

s.3 (9) of the BDSG defines ‘special categories of personal data’ as being “information on a person's racial and ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life.”

2.2.3.3 IP Addresses

While the discussions above²⁵¹ about whether IP addresses constitute personal data are still of some relevance in relation to Germany, more pertinent are a number of German court decisions on the subject. The most recent of these was taken by the Munich District Court on the 30th October 2008.²⁵² It ruled that dynamic IP addresses do not by themselves constitute personal data, as they cannot be linked to an identified or identifiable individual without the use of techniques which are both technically complex and illegal, whereby an ISP would have to transfer to a third party in possession IP addresses the logs which would allow to determine who was using a particular IP address at a certain time.²⁵³ This of course implies that in the hands of ISPs, who obviously possess this data, IP addresses do constitute personal data, and further that static IP addresses do too. Two earlier decisions

²⁴⁷ Balz, 2008, p7

²⁴⁸ Leyendecker, und Ott, 2009

²⁴⁹ S.3 No.3 TKG

²⁵⁰ Working Party 11, 2007, p.82

²⁵¹ Section 2.3.4

²⁵² 133 C 5677/08 (Kremer 2008)

²⁵³ Kremer, 2008.



taken by the Berlin Courts,²⁵⁴ took the opposite view, that IP addresses always constitute personal data, as rather than concentrating on the difficulty and illegality of acquiring the additional data needed to identify individuals, it merely observed that such data could be acquired, and therefore the individuals could be identified.²⁵⁵ These contradictory cases leave the status of IP addresses somewhat uncertain, and destined to remain so in the absence of a ruling by the Constitutional Court.

2.2.4 Processing of Personal Data

2.2.4.1 Definition

Processing is, according to s.3 (4) of the BDSG “the storage, modification, transfer, blocking and erasure of personal data. The meaning of these five words are then further elucidated; ‘storage’ as “the entry, recording or preservation of personal data on a storage medium so that they can be processed or used again, ‘modification’ as the alteration of the substance of stored personal data, ‘transfer’ as “the disclosure to a third party of personal data stored or obtained by means of data processing either a) through transmission of the data to the third party or b) through the third party inspecting or retrieving data held ready for inspection or retrieval,” ‘blocking’ as “labelling stored personal data so as to restrict their further processing or use,” and ‘erasure’ is stated to mean “the deletion of stored personal data.” The technological neutrality of these definitions is stressed in the phrase “irrespective of the procedures applied” which precedes the five more detailed definitions.

‘Collection’ is defined separately in s.3 (3) as “the acquisition of data on the data subject,” and in s.3 (5) ‘Use’ is defined incredibly broadly and somewhat tautologously, as “any utilisation of personal data other than processing.” The presence of these two alternative definitions outside of the definition of processing is unusual, as in the DPD and most of the laws implementing it collection and use are held to be types of processing. The BDSG is structured like this as of course it is not an implementation of the DPD but predates it, and therefore has its own structural logic. The importance of this distinction is that when considering the principles and rules governing data protection in the rest of the act it is imperative to pay attention to whether they apply to processing, collection and use or only one or two of these three activities.

There is an important distinction between processing and ‘automated processing,’ the performance of which results in the data controller being subject to a number of additional duties, such as the need to appoint a Data Protection Official,²⁵⁶ and to notify the relevant supervisory authority that it is being performed.²⁵⁷ S.3 (2) defines ‘automated processing’ as “the collection, processing or use of personal data by means of data processing systems. A non-automated filing system is any non-automated collection of personal data which is similarly structured [to an automated system] and which can be accessed and evaluated according to specific characteristics.” The concept of automated processing is therefore different here, not only because it is automated, but also because it includes the collection and use of data too.

²⁵⁴ That taken by the LG Berlin on the 6th September 2007, (23 S 3/07), which affirmed an earlier judgment by the AG Berlin (5 C 314/06) (Ulbricht, 2008).

²⁵⁵ Ulbricht, 2008

²⁵⁶ See section 3.4.2.5 below ‘Data Protection Officials.’

²⁵⁷ S.4d BDSG. See section 3.4.3 below ‘Data controllers’ duties.’



2.2.4.2 Relevant parties

2.2.4.3 The distinction between public and private bodies.

The distinction between public and private bodies in German law is significant as the two are subject to different regulatory regimes. Public bodies are subject to Part II of the BDSG, which decrees in some detail under what conditions it is legitimate to collect, store modify and use personal data, when it is permissible to transfer personal data to other public and private bodies and how data protection legislation should be implemented in the federal administration. Part II also grants the data subject additional rights in relation to public bodies. However as this report is concerned with what rules apply to research projects such as PICOS, it will focus on the rules applicable to private bodies, which are found in Part III of the BDSG, and explored in detail below in section 2.2.4.10 'Data protection principles.'

Private bodies are, according to s.2 (4) of the BDSG, "natural or legal persons, companies and other private-law associations." It adds that, "to the extent that a private body performs sovereign public administration duties; it shall be treated as a public body for the purposes of this Act." Conversely, in s.27, which defines the scope of Part III, it is made clear that the rules which apply to private bodies also apply to the public bodies of the Federation and the *Länder* "in so far as they participate in competition as public-law enterprises."²⁵⁸

In relation to private bodies the BDSG is applicable, according to s.1 (2), to the processing and use of personal data, by means of data processing systems, to the use or processing of personal data from or in non-automated filing systems, and to the collection of data for either of these types of system. However the scope of the additional rules applicable to private bodies in Part III is subtly different; s.27 states that they do not apply "to the processing and use of personal data outside of non-automated filing systems in so far as they are not personal data clearly taken from an automated processing operation." This caveat appears to mean that while Part III still covers the processing of data within non-automated systems, it does not extend as far as to cover the processing of personal data taken from such systems.

Public bodies are defined in s.2 of the BDSG as "the authorities, the bodies of the judicature and other public-law institutions, of the Federation, of the Federal corporations, establishments and foundations under public law as well as of their associations"²⁵⁹ or of the *Länder*, of the municipalities, an association of municipalities or other legal persons under public law subject to Land supervision as well as of their associations."

2.2.4.4 Data Controllers

A Data controller is, according to s.3 (7) of the BDSG, "any person or body collecting, processing or using personal data on his or its own behalf or commissioning others to do the same." The BDSG

²⁵⁸ Though, federal public bodies engaging in competition are still subject the oversight of the BfDI rather than the same supervisory authorities as private bodies (BDSG s.27 (1)).

²⁵⁹ S.2 also makes it clear that as long as they have an exclusive right to provide a postal service, the successor companies created from the Special Fund Deutsche Bundespost are considered public bodies.



applies to data controllers established in Germany and those from other EEA Member States if they collect, process or use personal data in a branch in Germany.²⁶⁰

As ‘Section 2.2.4.9 Data controllers’ duties’ below shows the responsibility for conforming to the law falls on the data controller.

2.2.4.5 Data Processors

The status and legal duties of the processor, in Art.2 (e) of the DPD are dealt with in s.11 in the context of an agent and principal relationship. S.11 (1) states that where other bodies, meaning processors “are commissioned to collect, process or use personal data, responsibility for compliance with the provisions of this Act and with other data protection provisions shall rest with the principal,” meaning the data controller. This is reasonable as the agent may only collect, use or process data as instructed by the principal.²⁶¹ It goes on to state that the rights of the data subject remain enforceable against the principal not the agent.

According to s.11 (2) of the BDSG the commission from the principal to the agent must be recording in writing, which specifies the scope, type and purpose of the handling of the data and the technical and organisational measures being taken to ensure data protection laws are adhered to. Furthermore the principal must verify compliance with these technical and organisational measures by the agent.²⁶²

The only duties applicable to the agent are these; to inform the principal if he thinks that the instructions given by the principal infringe the data protection laws,²⁶³ to respect the principle of confidentiality in s.5, to adopt the appropriate technological and organisational measures required by s.9 and in the case of private bodies also the duties relating to the appointment and responsibilities of data protection officials in s.4f and s.4g.²⁶⁴ Agents who are private bodies also remain subject to the authority of the *Länder*’s Data Protection Commissioners.²⁶⁵

2.2.4.6 Data Subjects

The definition of data subject is found within the definition of personal data, it is the “identified or identifiable individual,” and it is to the data subject that the rights found in section 2.2.7 below attach.

2.2.4.7 Data Protection Officials

German law goes to relatively extensive lengths to decree exactly how data protection rules should be enforced²⁶⁶ and symptomatic of this is the creation of the role of Data Protection Official (DPO) in s.4f

²⁶⁰ S.1 (5) BDSG

²⁶¹ S.11 (3) of the BDSG

²⁶² This degree of detail in the written commission was introduced in the reforms this year. (Schweinoch, 2009, p. 3)

²⁶³ S.11 (3) of the BDSG

²⁶⁴ The only offences for which an agent can be found responsible are these: s43 (1), Nos. 2, 10 and 11, (2) Nos. 1 to 3 and (3) and Section 44 (s.11 (4) BDSG).

²⁶⁵ S.11 (4) BDSG

²⁶⁶ This is also discernable in section 3.4.4.2, where technological and organisational measures are discussed.



D7.1a User Evaluation Plan

of the BDSG. Furthermore, recent scandals in Germany have led to changes in the law which strengthen the position, and increase the prevalence, of DPOs.²⁶⁷

Private bodies,²⁶⁸ which generally deploy more than 9 people to process personal data automatically must appoint a DPO, and those which permanently employ 20 persons or more to do so must also appoint one, whether the processing is automated or not.²⁶⁹ Furthermore, private bodies which carry out automated processing operations which process personal data in the course of business for the purposes of transfer or anonymised transfer are to appoint a DPO irrespective of the number of persons employed in the automatic processing of personal data,²⁷⁰ and under the new rules coming into effect on the 1st September 2009 so must any private body processing data for the purposes of market research.²⁷¹ Where there remains no obligation to appoint a DPO at a private body, the head of the private body is responsible for discharging the DPO's duties.²⁷²

The DPOs themselves must “possess the specialised knowledge,...have demonstrated the reliability necessary for the performance of the duties,”²⁷³ be free to use his specialised knowledge in the area of data protection and “suffer no disadvantage through the performance of his duties.”²⁷⁴ The reforms have fleshed out this last provision, stating that during their term of office, and for one year thereafter, DPOs may only be dismissed for good cause.²⁷⁵ However, if the DPO does not possess the specialised knowledge and demonstrate the reliability necessary for the performance of his duties, the relevant supervisory authority may demand his dismissal.²⁷⁶ Furthermore, employers must provide DPOs with assistants, premises, furnishings, equipment and other resources as necessary for the performance of their duties,²⁷⁷ and also now pay for their training.²⁷⁸

The unifying duty of the DPOs is to “work towards ensuring compliance” with data protection laws, especially by “[monitoring] the proper use of data processing programs with the aid of which personal data are to be processed,” and by taking suitable steps to familiarise the persons employed in the processing of personal data with data protection law.²⁷⁹ To be able to do this, the law states that they must be free to consult with the relevant supervisory authority,²⁸⁰ be informed in good time of projects involving the automatic processing of personal data,²⁸¹ have made available to them by the data

²⁶⁷ Schweinoch, 2009, p. 1

²⁶⁸ The rules applying to private bodies do still apply to telecommunications providers, as though they are monitored by the BfDI like a public body, they themselves are still private bodies.

²⁶⁹ S.4f (1) BDSG

²⁷⁰ S.4f (1) BDSG

²⁷¹ Schweinoch, 2009, p.1

²⁷² S.4g (2a) BDSG

²⁷³ S.4f (2) BDSG

²⁷⁴ S.4f (3) BDSG

²⁷⁵ Schweinoch, 2009, p. 1. This gives them the same protections afforded to employee representatives.

(Schweinoch, 2009, p. 1)

²⁷⁶ S.38(5) and s.4f (3)

²⁷⁷ S.4f (5) BDSG

²⁷⁸ Schweinoch, 2009, p. 1

²⁷⁹ S.4g (1) BDSG

²⁸⁰ S.4g (1) BDSG. The BfDI in the case of telecommunications undertakings and the appropriate *Land* Data Protection Commissioner in the case of other private bodies.

²⁸¹ S.4g (1) BDSG



controller an “overview of the information stipulated in the first sentence of Section 4e and a list of persons entitled to access,”²⁸² and that employees must be able to approach them with concerns about data protection at any time.²⁸³ It should also be noted that DPOs are bound to keep secret personal data that they are exposed to in their work,²⁸⁴

DPOs are also the party responsible for performing ‘prior checks’ on automatic processing systems to check that they are compliant with data protection law.²⁸⁵ They must do this where automated processing operations involve risks for the rights and liberties of the data subject, which is considered to be the case when special categories of personal data to be processed, or the processing of personal data is intended to appraise the data subject's personality, including his abilities, performance or conduct.²⁸⁶ Though this is not necessary where there is a statutory obligation to do the processing, where the data subject's consent has been obtained or the collection, processing or use serves the purposes of a contract or a quasi-contractual fiduciary relationship with the data subject.²⁸⁷

2.2.4.8 *The parties of the TKG*

The terms used to refer to the various parties involved in the trade of electronic communications services governed by the TKG are somewhat different to those used in the more general legislation of the BDSG. The terms used will be briefly outlined here. A ‘service provider’ means a person,²⁸⁸ who, on a wholly or partly commercial basis, provides a telecommunications service, or contributes to the provision of such a service,²⁸⁹ and a “subscriber” is a person who is party to a contract with a provider of telecommunications services for the supply of such services.²⁹⁰ This means that in the vast majority of cases the service provider will also be the data controller and the subscriber will also be the data subject, within the meanings of the BDSG. Additionally a ‘user’ is a natural person using a telecommunications service for private or business purposes, without necessarily having subscribed to that service,²⁹¹ such as a subscriber’s spouse, children or friends.

2.2.4.9 *Data controllers’ duties*

Data controllers are responsible throughout German data protection law for ensuring that the rules are adhered to and it is they who are liable to be punished both administratively and criminally if they

²⁸² S.4g (2) BDSG. This information is described below in section 3.4.3 ‘Data Controller’s Duties,’ as it consists of the information that must be included in an obligatory registration with a data protection commissioner. It is also notable that the Data Protection official must in turn make this information available to anyone, apart from the general description enabling preliminary assessment as to whether the measures to guarantee the safety of processing are adequate.

²⁸³ S.4f (5) BDSG

²⁸⁴ S.4f (4). They may be released from this obligation by the data subject.

²⁸⁵ S.4d (6) BDSG

²⁸⁶ S.4d (5) BDSG.

²⁸⁷ S.4d (5) BDSG.

²⁸⁸ In these translations from German unless otherwise indicated the word ‘person’ is intended mean both natural and legal person, as it does in the context of UK law..

²⁸⁹ S.3 No. 6 TKG

²⁹⁰ S.3 No. 20 TKG

²⁹¹ S.3 No. 14 TKG



breach those provisions.²⁹² They may also be civilly liable for any damage caused to the data subject due to the collection, processing or use of their personal data in breach of data protection laws, if they have not exercised due care.²⁹³

Subject to certain caveats, whenever a data controller puts automated processing procedures into operation they must in the case of private bodies notify the appropriate Data Protection Commissioners of the *Länder*, and in the case of telecommunications operators and service providers notify the BfDI.²⁹⁴ This notification must contain the name and address of the controller, the identities of the owners and managers in charge of the processing, and descriptions of the purposes for which personal data is being collected, processed or used, of the groups of data subjects and of the categories of data being processed.²⁹⁵ It must also detail the standard periods for the erasure of data, whether any data transfers in third states are planned, as well as include a general description enabling a preliminary assessment as to whether the measures to guarantee the safety of processing are adequate.²⁹⁶ However, as long as the undertaking is not performing automated processing for the purpose of transfer or anonymised transfer, such notification is not necessary where the undertaking concerned has a DPO,²⁹⁷ or where the undertaking collects, processes or uses personal data only for its own purposes, employs less than nine employees to do so and has obtained either consent from the data subject “or the collection, processing or use serves the purposes of a contract or a quasi-contractual fiduciary relationship with the data subject.”²⁹⁸ Failing to notify when it is obligatory is an administrative offence that may be punished in the manner detailed above in section 2.2.2.3 ‘Data Protection Commissioners of the *Länder*.’

The data controllers duties of notification *vis-à-vis* the data subject are described below in section 2.2.7, ‘Rights of the Data Subject.’

2.2.4.10 Data protection principles

The structure of the BDSG is very different to the DPD, and to most of the laws which implement the DPD in Europe, as rather than being an implementation of it, the BDSG predated the DPD and was modified in order to be compliant with it.²⁹⁹ Most significant in terms of the implementation of the principles ‘relating to data quality’ found in Art. 6 of the DPD, and the ‘criteria for making data processing legitimate’ of Art. 7 of the DPD, is that the provisions which correspond to them in the BDSG do not necessarily apply to the concept of processing native to the DPD. Rather they sometimes only apply to one of the three distinct activities of collecting, processing and using distinguished in the BDSG, or only to ‘transfer’ a subcategory of processing. Furthermore, for the large part, the principles

²⁹² The limited duties of Data Processors are outlined above in section 3.4.2.3 ‘Data Processors.’

²⁹³ S.7 BDSG. Data controllers’ supporting organisations may also be liable (S.7 BDSG).

²⁹⁴ S.4d (1) BDSG

²⁹⁵ S.4e BDSG

²⁹⁶ S.4e BDSG

²⁹⁷ S.4d (2) BDSG. This is logical as the data which becomes publically available through notifying the Data Protection Commissioners of the *Länder* will, where there is a DPO, be available from them.

²⁹⁸ S.4d (3) BDSG.

²⁹⁹ Direct comparisons between these sections and their counterparts dealing with the UK are therefore not entirely straightforward.



which govern private and public bodies are separate. Unsurprisingly the resulting body of law is somewhat complex.

2.2.4.11 General principles

S.3a describes the principles of data reduction and data economy, in which the BDSG goes considerably further than EU law requires in its closest corresponding provision, Art. 6 (1)(c) of the DPD. Furthermore, this is a provision that has been considerably broadened in the reforms this year, as while it used to only apply to the designing and selection of data processing systems, it now covers data collection, processing and use generally.³⁰⁰ It states that as little personal data as possible should be processed, collected and used and that wherever possible the possibilities for ‘aliasing’ and ‘rendering persons anonymous’ must be taken wherever technically possible, as long as the effort involved is reasonable in relation to the desired level of protection. The importance of doing this is stressed particularly in relation to data being collected or processed for market or opinion research purposes.³⁰¹ ‘Rendering anonymous’ is defined in s.3 (6) as “the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual and according to s.3 (6a) ‘Aliasing,’ sometimes known as ‘pseudonymisation,’³⁰² means replacing a person's name and other identifying characteristics with a label, in order to preclude identification of the data subject or to render such identification substantially difficult.

The principle of confidentiality is outlined in s.5. It is decreed that persons employed in data processing shall not collect, process or use personal data without authorisation and that such persons who work in the private sector must give a signed undertaking that they will observe this principle, both while employed by the data controller and thereafter.

The counterparts of the technical and organisational measures found in Art 17 of the DPD are found in s.9 of the BDSG. All bodies processing personal data must take all technical and organisational measures necessary to ensure the implementation of the provisions of the BDSG, as long as the effort involved is reasonable in relation to the desired level of protection. S.9 then draws attention to the annex of the BDSG in which a number of specific data protection measures are described. Briefly these are, preventing unauthorised persons from gaining access to data processing systems, preventing data processing systems from being used without authorization, ensuring that persons using a data processing system can only access the data to which they have a right of access, ensuring personal data cannot be read, copied, modified or removed without authorisation and ensuring that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed. Where processing or collection is performed by an agent s.11 (2) of the BDSG states that they should be carefully selected, with particular regard for the suitability of the technical and organisational measures taken by him.

Under s.6a it is made clear that decisions which have legal consequences for, or substantially impair the interests of the data subject must not be based exclusively on the automated processing of personal data which evaluates individual personal characteristics. However there is an exception to this rule

³⁰⁰ Schweinich, 2009, p. 2

³⁰¹ Schweinich, 2009, p. 10

³⁰² Schweinich, 2009, p. 2



where the decision is taken in relation to a contract with the data subject, the data subject is aware of the decision and the data subject's interests are protected by appropriate measures.

This year's amendments to the BDSG include new duties which make it obligatory to inform the regulatory authority and the data subject in the event of the abuse or loss of data falling within the 'special categories of data,' if it has the potential to seriously impair the data subject's rights or interests worthy of protection.³⁰³

2.2.4.12 General criteria that render the processing, use and collection of personal data legitimate

The BDSG proceeds from the assumption that the collection, processing and use of personal data is not legitimate and that a justificatory ground must be demonstrated.³⁰⁴

In relation to collection consent is one such justificatory ground.³⁰⁵ The detail of what exactly constitutes consent is elucidated in the BDSG, as it is in Art. 2 (h) of the DPD. S.4a states that consent consists of a free decision made by a data subject who is informed about the purpose of collection, processing or use and of the consequences of withholding consent. There is a presumption that consent should be given in writing, and until the most recent reforms the BDSG went on to state that "it must be made distinguishable in its appearance."³⁰⁶ This provision was admittedly vague and this year's reforms have been designed to remedy this. It has been clarified and it is now clear that a term granting consent may not be hidden in general 'Terms and Conditions,' but that "an express and typographically prominent arrangement of the declaration of consent is required."³⁰⁷ As regards the medium of consent, it may be electronic. S.94 of the TKG states that consent may be given electronically where it is given deliberately and unequivocally. It must also be recorded, the subscriber or user must be able to access his declaration of consent at any time and the subscriber or user must be able to withdraw his consent at any time with effect for the future.

Importantly for research projects such as PICOS there is an unusual exception in relation to consent. S4a (2) states that where the defined purpose of the research would be "impaired considerably if consent were obtained in writing," it shall be sufficient to record in writing the information that would normally have been given to the data subject along with an explanation of why in this circumstance obtaining consent would have compromised the aim of the research.

In the absence of consent it is possible to collect data from the data subject if a legal provision prescribes or presupposes such collection, if the nature of the administrative duty to be performed or the business purpose necessitates collection of the data from other persons or bodies, or if collection would necessitate disproportionate effort and there are no indications that overriding legitimate interests of the data subject are impaired.³⁰⁸

³⁰³ These provisions can be found in the new section, s.42a. (Schweinoch, 2009, p. 5)

³⁰⁴ s.4 (1) BDSG

³⁰⁵ s.4 (1) BDSG

³⁰⁶ S.4a (1) BDSG. It should be noted that consent is subtly different in relation to special categories of data, discussed below in section 2.2.4.17 'Processing special types of personal data.'

³⁰⁷ Schweinoch, 2009, pp.3-4

³⁰⁸ S.4 (2) BDSG



2.2.4.13 Criteria that render the processing, use and collection of personal data legitimate that are specific to private bodies

In Parts II and III, there are a plethora of other ways to render data processing, collection and use legitimate, though this report will only examine those in Part III, which apply to private bodies, not those in Part II, which are applicable to public bodies. Before the rules governing data processing in Part III are examined, it should be made clear that certain categories of data may under no circumstances be transferred to third parties or processed for purposes other than those it was gathered for, as other personal data may be if certain conditions found in s.28-30 are fulfilled. Most important to the PICOS project in this regard is s.40 as it concerns the “processing and use of personal data by research institutes” stating that “personal data collected or stored for scientific research purposes may be processed or used only for such purposes.” S.31 makes it clear that this is also the case in relation to data stored exclusively for the purposes of data protection control or data security or to ensure the proper operation of a data processing system and s.39 states that it is also the case in relation to data “subject to professional or special official secrecy and which have been supplied by the body bound to secrecy in the performance of its professional or official duties.” A new section, s.30a, adopted in this year’s reforms also outlines similar limits. It states that data collected for a specific research project which is not from generally accessible sources and data collected or stored for market or opinion research purposes may only be processed or used for their original purposes, unless it has been rendered anonymous.³⁰⁹ While it is not impossible to justify the transfer, or use for other purposes, of data subject to telecommunications privacy, the provisions which do so must make specific reference to telecommunications activities, which unsurprisingly the large majority do not.³¹⁰

The processing, use and collection of personal data for ‘own business purposes.’

S.28 describes the principles that private bodies are bound to respect when processing collecting or using personal data for their ‘own business purposes,’ which the BDSG stresses should be stipulated in concrete terms.³¹¹ Such processing is permissible where it is in accordance with the purposes of a contract or a quasi-contractual fiduciary relationship with the data subject, it is necessary to safeguard justified interests of the controller and the data is generally accessible or the data controller would be entitled to publish it.³¹² However, the processing, collection and use of data will be illegitimate if the data subject has a legitimate interest in his data being excluded from processing or use or collection, which outweighs the justified interest the data controller, is attempting to safeguard.³¹³ Whether the processing, use and collection of personal data for ‘business purposes’ is legitimate will therefore often come down to a balancing exercise between the two interests. Since this involves the restriction of a fundamental right, that of privacy, it is arguable that it is appropriate to consider the extensive jurisprudence of the ECJ and ECtHR, concerning the proportionality of such restrictions, when deciding whether a restriction is legitimate.

³⁰⁹ Schweinoch, 2009, p.2

³¹⁰ See section 3.8 ‘Confidentiality of Communications’ below.

³¹¹ This is effectively a detailed equivalent of the criterion for making data protection legitimate found in Art. 7 (b) of the DPD.

³¹² S.28 (1) BDSG

³¹³ S.28 (1) BDSG



Under s.28 (2) transferring personal data or using it for an alternative purpose is legitimate, unless it is banned under the new s.30a, where it is necessary to safeguard the justified interests of the controller and the data is generally accessible or the controller of the filing system would be entitled to publish it, though there is no need in this case for a contractual or quasi-contractual relationship. The same rules relating to the balancing of interests apply in this scenario as in relation to s.28 (1), although here it is specifically stated that such an interest exists where the data concerns criminal or administrative offences and is known to the controller due to a contractual relationship.

However, under s.28 (3) there are also a number of other ways to justify transferring personal data or using it for an alternative purpose, which again will not apply if the data is subject to s.30a. Crucially for the PICOS project it is permissible if “necessary in the interest of a research institute for the conduct of scientific research,” as long as the scientific interest in conducting of the research project substantially outweighs the interest of the data subject in excluding the change of purpose or transfer and there is no other way to achieve the research purpose without disproportionate effort.³¹⁴ The use of the word substantially here obviously raises the degree of necessity needed to make use of this exception beyond that required for the other exceptions listed below, perhaps unjustly as it is certainly arguable that research purposes are more worthy than those of market or opinion research and advertising. It is also notable that the exception for research is equally applicable to special types of personal data.³¹⁵

Such transfer is also permissible where it is necessary to protect the justified interests of a third party, to avert threats to state security and public safety, to prosecute criminal offences or for purposes of advertising, and market or opinion research. The last of these possibilities is known as ‘the list privilege’ and until the 1st of September this year it allowed lists of data that did not include more data than the data subject’s membership of the group of persons on the list, their occupation or type of business, name and title, academic degrees, address and year of birth, to be transferred or used for alternative purposes, as long as there is no reason to assume that the data subject has a legitimate interest in his data being excluded from such activities.³¹⁶

Since it was large lists of personal data that were at the heart of the scandals concerning the sale of personal data that were so pivotal in bringing about the reforms this year, it is no surprise that they came under scrutiny in them. While there were suggestions it should be abolished completely, it was eventually only restricted.³¹⁷ Now personal data may only be transmitted for advertising purposes and used by the data recipient if the addressee of the advertising is able to clearly identify the body responsible for the use of the data, how they obtained the data and who collected it.³¹⁸ In addition, the body transmitting the data and its recipient are obliged to store information on the origin of the data and, in the case of the body transferring, the identity of the data recipient, for a period of two years

³¹⁴ S.28 (3) No. 4 BDSG. When read in conjunction with s.40 it becomes clear that while data collected for scientific research purposes may not be used for other things, in certain circumstances data gathered for other purposes may be processed for the purposes of research.

³¹⁵ S.28 (6) No. 4 BDSG

³¹⁶ S.28 (3) BDSG

³¹⁷ Schweinoch, 2009, pp. 4-5

³¹⁸ Schweinoch, 2009, pp. 4-5



following the transmission and to provide the data subject with this information.³¹⁹ The duties relating to the maintenance of records come into force later than the other provisions, on the 1st April 2010 and it should also be noted that as regards data collected before the 1st of September 2009, so called 'legacy data' the new rules will not apply in relation to market or opinion research until the 31st of August 2010 and until 31st of August 2012 in relation to advertising.³²⁰

It should be noted that the recipient of the data may process or use the data only for the purpose for which they were transferred, unless it can meet the criteria that allowed controllers to process, collect and use data under s.28 itself.³²¹

The collection storage and modification of personal data for the purpose of eventually transferring it

Where rather than collecting, storing and modifying information for its own business purposes an undertaking is doing so for the purpose of eventually transferring it, as companies involved in for example advertising, and market or opinion research often do, the rules governing it are to be found in s.29 of the BDSG. These are largely the same as in s.28, but in a number of ways more stringent. Firstly, it is also crucial to make it clear that such activities cannot be legitimised because they are being performed for research purposes as they can be under s.28. Such collection, storage and modification are only legitimate where there is no reason to assume that the data subject has a legitimate interest in excluding such transfer or has no such clear overriding interest and the data are retrievable from generally accessible sources or the controller would be permitted to publish them.³²² Furthermore, the recipients of such transfers must credibly prove a justified interest³²³ in gaining access to the data or the data must be compiled in lists compliant with the 'list privilege,' and must be being transferred for purposes of advertising or market or opinion research.³²⁴

However, where data are collected and stored in the course of business in order to transfer them in an anonymised form s.29 does not apply,³²⁵ however the modification of personal data that will be transferred in an anonymised form remains permissible only under the same conditions as govern it in s.29.³²⁶ The central principle in this scenario is rather that the "characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately," and only be combined with the rest of the information when necessary for storage or, notably, scientific purposes.³²⁷

³¹⁹ Schweinoch, 2009, pp. 4-5

³²⁰ Schweinoch, 2009, pp. 6

³²¹ S.28 (5) BDSG

³²² S.29 (1) BDSG.

³²³ The transferring body must record this reason and its credible justification. (S.29 (2) BDSG.)

³²⁴ S.29 (2) BDSG. Here too though there must be no reason to assume that the data subject has a legitimate interest in excluding such transfer.

³²⁵ S.30 (4) BDSG

³²⁶ S.30 (2) BDSG

³²⁷ S.30 (1) BDSG

2.2.4.14 Special provisions concerning data processing in certain fields

The most significant of these for PICOS are those found in s.40, which concerns the “processing and use of personal data by research institutes.” As well as stating that “personal data collected or stored for scientific research purposes may be processed or used only for such purposes,”³²⁸ it states that “personal data shall be rendered anonymous as soon as the research purpose permits this.”³²⁹ S.40 also requires, even more strictly, that until the data is rendered anonymous, that the characteristics which enable information concerning personal or material circumstances to be attributed to data subjects be stored separately, and only be combined with the information to the extent required by the research purpose. When publishing the results of research personal data may only be published if either they have the data subjects consent, or if it is “indispensable for the presentation of research findings on contemporary events.”³³⁰ These requirements are relatively strict even in relation to the treatment of processing for other purposes within German law, and therefore contrast with the treatment of data processing for research purposes in other member states, where the rules governing it are normally less restrictive than those governing processing for other purposes.

In both s.27. (1) and s.1 (2) No.3 of the BDSG it is made clear that processing effected solely for personal or family activities is entirely exempt from data protection law.

The many scandals described in the introduction relating to employers spying on employees have led to specific, and far reaching, rules being introduced, in s.32 of the BDSG, that govern data processing of personal data held by employers in which employees are the data subject. Amongst other things this new provision decrees that for the purposes of the employment relationship, personal data may now only be collected, processed or used to the extent that is necessary for its initiation, performance or termination.³³¹ Furthermore these amendments are applicable to all data, whether it is processed automatically or not, which will be a considerable burden for businesses as even notes written about an employee will have to be treated in accordance with all the rules governing the processing of personal data.³³² These reforms will enter into force on 1st April 2010.

Data processing by the media is also subject to specific rules, detailed in s.41 of the BDSG.

2.2.4.15 Principles relating specifically to the formation of contracts between telecommunications providers and subscribers

When concluding a contract with a subscriber, service providers are bound to inform their subscribers of certain statutorily mandated information in a readily comprehensible and non-technical way; this consists of the basic facts describing the extent, purpose and manner in which the collection, use and processing of personal data will take place.³³³ Particular attention must be drawn to choices and

³²⁸ See section 3.4.4.1 ‘General Principles.’

³²⁹ The concept of ‘rendering anonymous’ is elucidated in section 3.4.4.1 ‘General principles’ above.

³³⁰ S.40 (3)

³³¹ Schweinich, 2009, p.1

³³² Schweinich, 2009, p. 2

³³³ S.93 TKG



options permitted to the subscriber. Users must also be informed by the service provider about the collection and use of personal data, by means of generally available information.³³⁴

The service provider may collect and use customer data³³⁵ to the extent required achieving the aims of establishing, framing the contents of, modifying or terminating the contract.³³⁶ More specifically the TKG states that when establishing or modifying a contractual relationship the service provider may require presentation of an official identity card where this is necessary to verify the subscriber's particulars, which it may make a copy of. However, the copy is to be destroyed without undue delay once the subscriber's particulars have been established, and it may be used for no other purpose.³³⁷ Furthermore, "under a contractual relationship with another service provider, the service provider may collect and use the customer data of his subscribers and of the subscribers of the other service provider to the extent required for performance of the contract between the service providers," though transfers to other third parties are possible with the subscriber's consent or if justified by some other criteria.³³⁸ This exception for transfers between subscribers is of course necessary for the interconnection of different operator's networks.

It is also important to note that the provision of telecommunications services may not be made dependent upon the subscriber's consent to use of his data for other purposes where there is not a reasonable way in which the subscriber could access such telecommunications services in another way.³³⁹

Other rules relating to these contracts are to be found below in section 2.2.9 'Direct Marketing, and 2.2.10 'Data Retention.'

2.2.4.16 Principles specifically concerning media for the mobile processing of personal data

The huge potential for the growth of such media has led to the German legislature going beyond the confines of what is necessary to implement the DPD, creating specific rules for such 'mobile personal storage and processing media.' These devices are defined as those which are "storage media which are issued to the data subject, on which personal data can be processed automatically beyond the storage function by the issuing body or another body and which enable the data subject to influence this processing only by using the medium."³⁴⁰ The breadth of such a definition is considerable; as it ranges from mobile phones, perhaps the most ubiquitous of such devices to smart cards.³⁴¹ The data subjects' ability to use their rights of access must be free of charge,³⁴²

³³⁴ S.93 TKG

³³⁵ See section 3.3.1 'Definition.'

³³⁶ S.95 (1) TKG

³³⁷ S.95 (4) TKG

³³⁸ See sections 3.2.2.2 and 3.4.4.3 above.

³³⁹ S.95 (5) TKG

³⁴⁰ S.3 (10) BDSG

³⁴¹ Korff, 2004, p. 33

³⁴² S.6c (2)



The bodies, such as telecommunications operators and shops, who issue such devices, and those which apply procedures for the automated processing of personal data which run on or work in conjunction with such devices, or who modify or make available data from such devices, must notify the device holder of certain information. Specifically their identity, address, what to do if they lose the device, a comprehensible explanation of what the device does, a description of what data the device processes, and how the user can exercise their rights of access to, and correction and erasure of data,³⁴³ and perhaps most importantly it must be clear to the data subject when such devices are performing data processing operations.³⁴⁴

In Germany there has been a considerable amount of publicity surrounding radio frequency identification (RFID) devices, which certainly qualify as media for the mobile processing of personal data, as they are a type of automatic identification system consisting of portable tags that enable data to be wirelessly transmitted to readers that process the data. They are for example used in the newest e-passports, which even contain digitised images of their owners faces that can be read via radio links,³⁴⁵ and certain shops, perhaps most famously Metro,³⁴⁶ have been including them in their loyalty cards. The BfDI had publically recognised the dangers RFID devices can pose for privacy, especially as they can easily be invisibly embedded in products.³⁴⁷ It has therefore stressed that data subjects must be fully aware of whether they are being issued with RFID devices and what processing the devices will do and that the devices must be capable of being entirely deactivated if the data subjects wish.³⁴⁸ Furthermore the BfDI has made it clear that using such devices to build up profiles on users' behaviour without the users consent is illegal.³⁴⁹

2.2.4.17 Processing special types of personal data

The provisions governing the processing of special types of personal data are not dealt with generally in the BDSG, but are dealt with entirely separately in relation to public and private bodies. Though it is a general rule that such data must be erased, and therefore cannot be processed or used, and should not have been collected, where the controller cannot prove its veracity.³⁵⁰ The latter half of s.28 contains the rules that bind private bodies when processing special types of personal data, which this report will concentrate on. There are a number of circumstances that can render the collection, processing and use of such data for an undertaking's 'own business purposes' legitimate, which correspond broadly to those in Art.8 (2) of the DPD. These also render collection, storage and modification, for the purpose of eventually transferring data, legitimate.³⁵¹ Apart from the exception for research purposes, which applies to special categories of personal data in the same way as to other

³⁴³ S.6c (1). These rights are discussed below in section 3.7 'Rights of the Data Subject.'

³⁴⁴ S.6c (3)

³⁴⁵ BfDI, 2006, p.31

³⁴⁶ Handel, 2005

³⁴⁷ BfDI, 2006, p.31

³⁴⁸ BfDI, 2006, pp. 32-33

³⁴⁹ Federal BfDI, 2006, p.33

³⁵⁰ S.35 (2) No. 2 BDSG

³⁵¹ S.29 (5) BDSG. S.30 (5) BDSG. States that the same rules also apply where the data is transferred in anonymised form.



personal data,³⁵² the most significant of these is the data subject's consent, which is defined slightly more strictly than the concept of consent outlined above in section 2.2.4.12; where special categories of personal data are concerned the consent must include a statement to the effect that it is specifically consent to process this type of data.³⁵³ Such processing, collection and use will also be legitimate where it is vital to protect the interests of the data subject or of a third party where the data subject is unable to give his consent for physical or legal reasons, the data concerned has already clearly been made public by the data subject or if it is necessary to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest to prevent such use, collection or processing.³⁵⁴

The collection processing and use of special types of personal data is also permissible for certain medical purposes if the processing is carried out by medical personnel or other persons who are subject to an obligation to maintain secrecy³⁵⁵ and to avert substantial threats to state security or public safety.³⁵⁶ It is also legitimate when it is performed by political, philosophical or religious organisations or trade unions, is necessary for that organisation's activities and concerns only the personal data of their members.³⁵⁷

It is also notable that the automatic processing of special types of personal data automatically requires the performance of prior checks, as described above in section 2.2.4.9 'Data controllers' duties.'

2.2.5 Traffic Data and its processing

Traffic data is defined very broadly as "data collected, processed or used in the provision of a telecommunications service."³⁵⁸ However the manner in which service providers are permitted to collect and use it is explained in considerable detail in s.96 of the TKG. Only the following specific types of traffic data may be collected, processed or used at all by service providers;

1. The number or other identification of the lines in question or of the terminal, personal authorisation codes, the card number when customer cards are used and location data when mobile handsets are used.
2. The beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted.
3. The telecommunications service used by the user.
4. The termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted.

³⁵² S.28 (6) No. (4) BDSG. Data may be transferred or used for an alternative purpose if it is "necessary in the interest of a research institute for the conduct of scientific research," as long as the scientific interest in conducting of the research project substantially outweighs the interest of the data subject in excluding the change of purpose or transfer, and there is no other way to achieve the research purpose without disproportionate effort.

³⁵³ S.4a (3) BDSG

³⁵⁴ S.28 (6) BDSG

³⁵⁵ S.28 (7) BDSG

³⁵⁶ S.28 (8) BDSG

³⁵⁷ S.28 (9) BDSG

³⁵⁸ S.3 No. 30 TKG



5. Any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.”

It is notable that location data is mentioned here, demonstrating that location data and traffic data do overlap, however rather troublesomely there does not appear to be any indication which set of provisions applies when data is both traffic data and location data.

The service provider can obviously collect, process and use such data to provide telecommunications services. Traffic data may be used after the termination of a connection only where required to set up a further connection, or for purposes related to billing,³⁵⁹ to detect faults in telecommunications, to detect fraud such as surreptitious use of services and other unlawful uses of telecommunications networks,³⁶⁰ and to provide subscribers that demonstrate they are the object of malicious or nuisance calls with data on the perpetrators.³⁶¹

Furthermore if the service provider obtains consent from the subscriber they may use subscriber-related traffic data for the purpose of marketing telecommunications services, shaping telecommunications services to suit the needs of the market or for the provision of value added services.³⁶² To use data about the called party their consent needs to be obtained separately. This consent must be informed, in that the consenter must be aware of the purposes for which their personal data will be processed, how long it will be retained for and that they have the possibility to withdraw it at any time.³⁶³

Before the implementation of the Data Retention Directive where there was no legal justification for retaining traffic data it had to be erased without undue delay following termination of the connection.³⁶⁴ This rule, by mentioning the termination of the call as the beginning of the time frame for deletion implied that it had to be done very quickly indeed, but now traffic data is subject to the rules on data retention and must be kept for 6 months, as is explained in more detail below in section 2.2.10 ‘Data Retention.’

2.2.6 Location Data and its processing

Location data is any “data collected or used in a telecommunications network, indicating the geographic position of the terminal equipment of an end-user of a publicly available telecommunications service.”³⁶⁵ The collection and use of location data is regulated in s. 98 of the TKG, which deals with it in rather strict terms, presumably because the potential for spying on others that comprehensive location data creates is so huge. Location data may only be processed if it has been

³⁵⁹ S.97 of the TKG contains the detailed provisions which deal with billing in general, and s.98 addresses how personal data must be dealt with in relation to itemised billing.

³⁶⁰ S.100 TKG

³⁶¹ S. 101 TKG

³⁶² A value added services are services which require the collection and use of traffic data or location data beyond that which is necessary for the transmission or billing of a communication’ (s 3 No. 5 TKG).

³⁶³ S.96 (4)

³⁶⁴ S.96 (2) TKG

³⁶⁵ s. 3 No. 19 TKG



anonymised,³⁶⁶ or where the ‘service provider’ has the consent of the subscriber. However even with the consent of the subscriber it may only be collected, processed and used to the extent, and for the duration, necessary for the provision of value added services.³⁶⁷ This consent may be withdrawn at any time, and the subscriber must also retain the possibility by “using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.”³⁶⁸ Interestingly it is explicitly stated that it is the subscribers’ duty to inform other users of the consent they have given to have the location data processed.³⁶⁹ The issue of the subscriber to an electronic service very often differing from its user plagues many aspects of electronic communications law, from liability for copyright infringements to the obtaining of appropriate consent, and while this may not completely solve it, it does at least address it.

The processing of location data is relatively widespread in Germany, being used to provide services as diverse as a buddy tracking system, automatic payment services, electronic bracelets for elderly disoriented persons and a GPS service for tracking children.³⁷⁰ However perhaps the most informative example to explore is that of “pay as you drive” car insurance, about which the BfDI has expressed concerns.³⁷¹ In such systems cars are equipped with an ‘on board unit’ which uses GPS to collect detailed information on driving behaviour, which insurance companies can then use to monitor the risks posed by particular drivers.³⁷² The BfDI appears to be uncomfortable with such technology on principle, as it is in his view a type of ‘Totalkontrolle,’ though he also points out a more specific problem relating to consent; with such systems it is very hard to be sure that the person who consented to the processing of the location data is always the same as the person actually driving, whose data is actually being processed.³⁷³

2.2.7 Rights of the Data Subject

The rights of the data subject are spelt out in the BDSG, and it is important to recognize that since there are not more specific provisions detailing them in the TKG, that these are also the rights afforded to telecommunications subscribers. S.6 of the BDSG makes it clear that German law gives considerable importance to the rights of the data subject, describing them as ‘inalienable.’ It goes on to clarify that the data subjects rights of access and to have data corrected, erased or blocked may not be restricted in any way by a contract.³⁷⁴

The data subject has a right to actively demand access to data, according to s.34. S.34 states that data subjects may request information on stored data concerning them, including what its provenance is,

³⁶⁶ Notably pseudonymisation is insufficient.

³⁶⁷ See footnote 414 above.

³⁶⁸ S.98 (2) TKG

³⁶⁹ S.98 (1) TKG

³⁷⁰ Working Party 11, 2007, p.77

³⁷¹ Schulzki, 2006

³⁷² Working Party 11, 2007, p.77

³⁷³ Schulzki, 2006

³⁷⁴ S.6 (1) BDSG



D7.1a User Evaluation Plan

the recipients or categories of recipients to whom it is transmitted and the purpose of storage.³⁷⁵ However, there are certain circumstances in which this right is not applicable, which crucially include when “storage or transfer is necessary for the purposes of scientific research and notification would require disproportionate effort,” and where providing information would require excessive work.³⁷⁶ The information provided should normally be given in written form,³⁷⁷ and in most circumstances free of charge.³⁷⁸ The BfDI has ruminated at some length on the difficulties of balancing the interests of undertakings, who may have to go to considerable lengths to meet these requests and data subjects who wish to access their data.³⁷⁹ He has encouraged data subjects to make their requests as specific as possible and for controllers not to brush requests off by giving out general descriptions of the data held, which do not allow the data subject to check its accuracy.³⁸⁰

The data subject has a right to insist upon the correction of incorrect personal data,³⁸¹ and if it cannot be ascertained whether or not it is correct it must be blocked.³⁸² Again though described as a right, this duty binds the controller whether or not data subject requests the correction. Similarly the data controller is bound to erase personal data, if their storage is not legitimate, they are from a special category of personal data and the data controller cannot prove their veracity or if their continued storage is not longer necessary.³⁸³ Where they are either legally prevented from erasing it, it is disproportionately expensive or difficult to do so or doing so could harm the legitimate interests of the data subject it must be blocked rather than erased.³⁸⁴ Furthermore it should be noted that if it is indispensable for scientific purposes, blocked data may be transferred or used without the consent of the data subject only, where the transfer or use of the data for this purpose would be admissible if they were not blocked.³⁸⁵ The behaviour of Google in relation to its ‘Street View’ project in Germany illustrates well the differences between erasure and blocking. In other countries people have been able to have personal data it collects, such as pictures of faces and licence plates, blurred by request, which is a form of blocking, but due to the strong protests the project has elicited in Germany Google has promised to delete the data entirely when requested to.³⁸⁶ Activists have demanded this as they consider blocking inadequate as while the blurred image is all that is publically, and if the law is strictly obeyed, privately seen, Google still possesses the unblocked original image.³⁸⁷ This again shows the strong emotions that issues of data protection give rise to in Germany.

³⁷⁵ As long as knowing the identities of the recipients, or the data’s origin, does not reveal a trade secret, which is an overriding interest.

³⁷⁶ S.34 (4) BDSG

³⁷⁷ S.34 (3) BDSG

³⁷⁸ S.34 (5) BDSG

³⁷⁹ BfDI, 2004, p.67

³⁸⁰ BfDI, 2004, p.67

³⁸¹ S.35 (1) BDSG

³⁸² S.35 (4) BDSG There is a definition of blocking in section 3.4.1 above, ‘Definition.’

³⁸³ S.35 (2) BDSG

³⁸⁴ S35 (3) BDSG. The rules described in this paragraph do not apply in certain circumstances described in s35 (5) which concern data from generally accessible sources.

³⁸⁵ S35 (8) BDSG

³⁸⁶ Schroeder, 2009

³⁸⁷ Schroeder, 2009



There are also a number of situations in which the data subject has a right to prevent collection, processing or use by filing an objection with the controller. This is the case when an examination, which the data controller must perform if an objection is made, reveals that the data subject's legitimate interest outweighs the controller's interest in such collection, processing or use.³⁸⁸ However, where the data is to be used or transferred for the purposes of advertising or of market opinion research, there is no need to balance their interests, the data subject's objection is automatically upheld.³⁸⁹ This objection must furthermore also be respected by third parties to whom the data is transferred.³⁹⁰ The enforceability of these provisions allowing the data subject to object to processing has been greatly enhanced by the reforms this year which oblige the body transmitting the personal data and its recipient to store information on the origin of the data and, in the case of the body transferring, the identity of the data recipient, for a period of two years following the transmission and to provide the data subject with this information.³⁹¹ Before these provisions came into force it could be very difficult to trace who was in possession of their personal data in order to exercise these rights

The BDSG also contains some 'rights of the data subject' which it is perhaps slightly strange to describe as rights, as they are effectively additional duties of the data controller. Where personal data are collected from data subjects, the controller must inform them as to the identity of the controller, the purposes of collection, processing or use and the categories of recipients. Unlike in the UK, no criterion of practicality has been introduced in Germany in relation to these principles from Section IV of Chapter II of the DPD. Though in circumstances where there are grounds for the data subject to assume that data will be transferred to certain recipients or they already have this knowledge there is no need to inform them of the recipient's identity.³⁹²

The data subject also has a more general right to be notified if personal data of which he is the subject are stored for the first time by an undertaking for its 'own purposes,' and he is not yet aware of it.³⁹³ Such data subjects have the right to be notified of the type of data involved, the purposes of collection, processing or use, the identity of the controller and the categories of recipients, in so far as the subject cannot be expected to assume transfer to such recipients.³⁹⁴ Furthermore, where data is being collected for the purposes of advertising or market or opinion research, the data subject shall be informed of their right to object to such use, as described below.³⁹⁵ There is, however, an extensive list of situations in which this duty is not applicable, most pertinent of which is when "storage or transfer is necessary for the purposes of scientific research and notification would require disproportionate effort."³⁹⁶ Other such situations include when the data are stored merely because they may not be erased due to legal statutory or contractual provisions on their preservation, when the data

³⁸⁸ S.35 (5) BDSG

³⁸⁹ S.28 (4) BDSG

³⁹⁰ S.28 (4) BDSG

³⁹¹ Schweinoch, 2009, pp. 4-5. This is also discussed above in section 3.4.4.3 'Criteria that render the processing, use and collection of personal data legitimate.'

³⁹² S.4 (2) BDSG This provision also states that where a data subject is legally obliged to provide data they must be informed of the consequences of not doing so.

³⁹³ S.33 (1) BDSG

³⁹⁴ S.33 (1) BDSG

³⁹⁵ S.28 (4) BDSG

³⁹⁶ S.33 (2) BDSG



are stored for the undertakings own purposes, are taken from generally accessible sources and notification is unfeasible on account of the large number of cases concerned and when the relevant authority has informed the data controller that publication of the data would jeopardise public safety.³⁹⁷

2.2.8 Confidentiality of Communications

Article 10 of the GG guarantees the Privacy of correspondence, posts and telecommunications, stating that it is inviolable, but that restriction may be ordered subject to the law as long as they serve to protect the free democratic basic order or the existence or security of Germany. S.88 of the TKG is a specific implementation of this principle, although unlike in its relation with the BDSG, the specificity of the TKG here does not remove the primacy of the GG, which remains superior due to its constitutional position. S.88 states that the content and detailed circumstances of telecommunications, including whether or not a person is or was engaged in a telecommunications activity or an unsuccessful attempt at one, shall be subject to ‘telecommunications privacy.’ Telecommunications privacy is a somewhat limited concept though as it only binds service providers,³⁹⁸ who are prohibited from procuring for themselves or others any information subject to telecommunications privacy other than that necessary for the commercial provision of their telecommunications services.³⁹⁹ Furthermore they may not process any data subject to telecommunications privacy for any other purpose, or pass it on to others unless such an action is provided for in a data protection law that refers explicitly to telecommunications activities.⁴⁰⁰ The various methods through which the processing of personal data can be rendered legitimate discussed above, in section 2.2.4.10 ‘Data protection principles,’ therefore do not apply to data subject to ‘telecommunications privacy,’ as those provisions do not expressly refer to telecommunications activities.

2.2.8.1 Interception

Section 89 of the TKG prohibits the interception of communications by everyone, whether or not they are a service provider and therefore subject to ‘telecommunications privacy.’ Where an interception occurs unintentionally the interceptor may not pass on the contents of the interception, or even the knowledge that it took place to, anyone. The only exceptions to this concern radio signals, which it is permissible to intercept if they are intended for the general public, radio amateurs or the operator of the radio equipment, and interceptions which have special legal authorisation, such as wiretaps authorised by a court.

Certain types of monitoring equipment are also forbidden. S.90 states that “it shall be prohibited to own, manufacture, market, import or otherwise introduce [to Germany] transmitting equipment which, by its form, purports to be another object or is disguised under an object of daily use and, due to such circumstances, is particularly suitable for intercepting...non-publicly spoken words ...or for taking

³⁹⁷ S.33 (2) BDSG

³⁹⁸ S.88 (2) TKG

³⁹⁹ S.88 (2) TKG. The provision of services includes the protection of the systems delivering them.

⁴⁰⁰ S.88 (3) TKG



pictures ... without...detection.”. However, certain state bodies are still allowed to use such equipment.⁴⁰¹

The provisions relating to the confidentiality of communications in Germany are criminally sanctioned, by a maximum of two years in jail.⁴⁰²

2.2.9 Direct Marketing

The principal provision concerning direct marketing in Germany is found in the Law against Unfair Competition, the *Gesetz gegen den unlauteren Wettbewerb* (UWG).⁴⁰³ S.7 of the UWG, which is titled 'unreasonable harassment,' makes it clear that any business act that results in someone being harassed unreasonably is outlawed, but advertising is explicitly mentioned as being a likely way this can happen. There is a presumption unreasonable harassment is taking place whenever, advertising is sent using an automated calling machine, a fax machine or by electronic mail without prior express consent of the addressee, phone calls are made for the purpose of direct marketing to consumers without their prior express consent⁴⁰⁴ and when such phone calls are made repetitively from a non-listed number. Furthermore direct marketing messages must clearly state the identity and address of the sender, and it must be possible for the recipient to be able to request that no more messages are sent without incurring costs greater than the base rates. It is also possible for a firm to directly market products or services by electronic mail that are similar to what a recipient has previously purchased, as long as it collected the personal data itself, the customer has not already objected to such marketing, and its clear in every message that the recipient can opt out at any time.⁴⁰⁵ Very interestingly it is also permissible for such adverts to contain 'enclosed advertising' provided by third parties and therefore an undertaking, as long as it also advertises services it provides itself, may include adverts from other undertakings, and all without consent.⁴⁰⁶ It seems likely that this could give rise to some interesting business models.

The specific rules for telecommunications service providers regarding direct marketing state that they may address text or picture messages to the telephone or postal address of their own subscribers unless the subscriber has objected, making it essentially an opt-out system in relation to their own customers.⁴⁰⁷ They may use the customer data of subscribers they have obtained through a contractual relationship with another service provider for direct marketing, as well as for 'subscriber advisory purposes' and market research, only to the extent required for such purposes and provided the subscriber has given his consent.⁴⁰⁸ This is therefore in contrast an opt-in system. Furthermore, when

⁴⁰¹ S.90 (1) TKG

⁴⁰² S.148 TKG

⁴⁰³ 7th June 1909 (RGI. P. 499), last modified on the 3rd August 2009 (Federal Law Gazette I, No. 49 of 03.08.2009, page 2413)

⁴⁰⁴ Consent may be implied where the recipient of the call is someone other than a consumer, such as a business (s.7 (2) UWG)

⁴⁰⁵ Schweinich, 2009, p. 4. S.7 (3) UWG

⁴⁰⁶ Schweinich, 2009, p. 4

⁴⁰⁷ S95 (2) TKG

⁴⁰⁸ S95 (2) TKG



the address or telephone number is collected it must be made clear that it is possible at any time to object to the sending of any more direct marketing messages.⁴⁰⁹

2.2.10 Data Retention

Although, currently the rules implemented by the Law on the revision of the telecommunications and other undercover investigative measures, also implementing Directive 2006/24/EC, *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/E*⁴¹⁰ are valid, the German law on data retention is in a state of some confusion at the moment. The Administrative Court of Wiesbaden, in decision 6 K 1045/08.WI of the 27th February 2009,⁴¹¹ has ruled that to retain data recording all internet and telephone usage is disproportionate in its breaching of the right to privacy.⁴¹² The court has referred to the ECJ the question of whether the Data Retention Directive is compatible with the principle of privacy or a disproportionate restriction of it.⁴¹³ This will be the second time that the directive has gone before the ECJ as on the 10th February 2009 in case C-301/06, Ireland and Slovenia's claim that it was adopted on an incorrect legal basis was dismissed.⁴¹⁴ However, the court was careful on that occasion to stress that this ruling had no relevance to whether or not the directive was compatible with fundamental rights.⁴¹⁵ There is considerable public disapproval of the new laws on data retention, which has manifested itself in large protests.⁴¹⁶ The Bundesrat has also stated that it believes that the current level of data retention violates the German constitution,⁴¹⁷ as has the BfDI, who has done so in very strong terms. Peter Schaar argues that blanket data retention affects the rights of a huge number of innocent people while most of those whom it is intended to target are well enough versed in techniques to circumvent monitoring that they will not be affected, and that it lacks entirely any sense of proportionality whereby there is some sort of correlation between the risk someone poses and the degree to which they are monitored.⁴¹⁸ Finally it should be noted that a couple of recent decisions⁴¹⁹ by the District Court of Bavaria and Thuringia have restricted considerably the ability of the police to make use of retained data, which appears to further demonstrate a systemic distaste for the laws stemming from the Data Retention Directive. Although neither the ECJ nor the German Constitutional Court has yet ruled on data retention with regard to human right and mainly the right to privacy, it does seem that the tide is turning against these laws requiring blanket data protection.

However, as the laws on data retention are still binding, they will now be described. The traffic data that service providers must retain consists of, in relation to fixed and mobile telephony, the calling and

⁴⁰⁹ S95 (2) TKG

⁴¹⁰ 21st December 2007 (No. 70, 31.12.2007, p. 3198)

⁴¹¹ This decision has been made available online in its entirety by 'Stoppt die Vorratdatenspeicherung,' at <http://www.vorratsdatenspeicherung.de/content/view/301/1/lang.de/>

⁴¹² Stoppt die Vorratdatenspeicherung, 2009

⁴¹³ Stoppt die Vorratdatenspeicherung, 2009

⁴¹⁴ BfDI, *Tätigkeitsbericht zum Datenschutz für die Jahre 2007 und 2008*, 2009, p. 33

⁴¹⁵ BfDI, *Tätigkeitsbericht zum Datenschutz für die Jahre 2007 und 2008*, 2009, p. 33

⁴¹⁶ Krempf, 2008

⁴¹⁷ Bundesrat, 2009

⁴¹⁸ BfDI, *Tätigkeitsbericht zum Datenschutz für die Jahre 2007 und 2008*, 2009, p. 32

⁴¹⁹ Those of the 11th March 2008 (1 BvR 256/08) and 28th October 2008 (1 BvR 256/08).



D7.1a User Evaluation Plan

receiving telephone numbers, the names and addresses of the subscribers or registered users of the aforementioned numbers, the date and time of the start and end of the call and the telephone service used. In relation to mobile telephony this additional information must also be retained; the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI) of the telephone calling and receiving telephones, the cell ID at the start of the communication, data identifying the geographic location of cells by reference to their cell ID, and if it is a pre-paid anonymous service, the date and time of the initial activation of the service and the cell ID from which the service was activated.⁴²⁰ In relation to internet access, internet e-mail or internet telephony, the following must be retained; the user ID allocated, the user ID and telephone number allocated to the communication entering the public telephone network, the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication, the date and time of the log-in to and log-off from the internet access service, the IP address, the user ID of the subscriber or registered user of the internet access service, in the case of dial-up access, the calling telephone number or in other cases, the digital subscriber line (DSL) or other end point of the originator of the communication. In the case of internet telephony, the user ID or telephone number, and the name and address of the subscriber of the intended recipient of the call must also be retained. In the case of e-mails, the name or registered user and the user ID of the intended recipient of the communication, and the date time and duration of the login to the e-mail service must also be held.⁴²¹

It is only required that this data be stored for the minimum period allowed in the Data Retention directive, 6 months,⁴²² and nor may it be stored for much longer as the service provider is bound to have erased the data within a month of it no longer having to be retained.⁴²³ Other provisions make it explicitly clear that communication and data accessed via web pages may not be saved because of these provisions,⁴²⁴ and that technical and organisational measures must be taken to ensure that access to the stored data is only possible by specially authorised persons.⁴²⁵ Bearing in mind the fact that with these extra provisions, and the 6 month retention period the German transposition is probably one of the less authoritarian in Europe, it is interesting to see what a huge outcry it has produced. It only goes to prove that these issues are still very sensitive in Germany.

Certain other provisions also deal with data retention. S.95 (3) of the TKG allows for a longer period of retention stating; “when the contractual relationship ends, the customer data are to be erased by the service provider upon expiry of the calendar year following the year in which the contract terminated.” Additionally when proof of identity is required to initiate a contract between a subscriber and a service provider, copies of official identity documents, must be destroyed without undue delay once the subscriber’s particulars have been established, and they may be used for no other purpose.⁴²⁶

⁴²⁰ S.113a TKG (2)

⁴²¹ S.113a TKG (3)-(4)

⁴²² S.113a TKG (1)

⁴²³ S.113a TKG (11)

⁴²⁴ S.113a TKG (8)

⁴²⁵ S.113a TKG (10)

⁴²⁶ S.95 (4) TKG



However, where more specific provisions do not apply the provision which deals with data retention remains s.3a of the BDSG which expounds the principle of data economy, and therefore requires that data be retained for no longer than necessary.

2.2.11 Conclusion

Germany is not dissimilar to the UK in that data protection is a subject upon which the public are relatively well versed, and therefore, if a negative public reaction is to be avoided, it is important to be careful not to breach data protection laws. However the German authorities seem far more predisposed to support data protection initiatives, than those in the UK, as a number of court decisions, and the opinions of the BfDI show.

2.3 Conclusion

This analysis delineates the basic legislation that will apply to a commercial application of the PICOS system. It contains the basic provisions that will need to be respected. This analysis has illustrated that although the European legal framework on data protection sets out the basic rules and principles that need to be respected regarding privacy and identity management, there may be significant differences in the national legal frameworks of various Member States, where the PICOS project may be commercially deployed. It is imperative to obey data protection laws as they are the embodiment of the human right to privacy, and in both the UK and Germany there is also a substantial risk of a public backlash in cases in which they are not respected. Further, in Germany such breaches are likely to expose the transgressor to the risk of prosecution, though this is a less likely consequence in the UK.

2.4 Bibliography & References

Arthur, C., 'Phorm fires privacy row for ISPs,' *The Guardian*, 6th March 2008, online at <http://www.guardian.co.uk/technology/2008/mar/06/internet.privacy>, last checked 20/08/2009

Bainbridge, D., and Pearce, G., 'Tilting the Windmills - Has the New Data Protection Law failed to make a Significant Contribution to Rights of Privacy', *The Journal of Information, Law and Technology (JILT)*, 2000 (2), online at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/bainbridge, last checked 7/07/2009

Balz, M., 'Datenschutzbericht 2008,' Deutsch Telekom, online at http://www.download-telekom.de/dt/StaticPage/65/62/44/090428_DTAG_Datenschutzbericht_656244.pdf, last checked 11/09/2009

Bartsch, M., Dohmen, F., Pauly, C., Reuter, W., and Schiessl, M., 'Im Netz der Späher,' 8th June 2008, *Der Spiegel*, online at <http://wissen.spiegel.de/wissen/dokument/dokument.html?titel=Im+Netz+der+Sp%C3%A4her&id=65640663&top=SPIEGEL&suchbegriff=deutsche+telekom+datenschutz&quellen=&qcrubrik=wirtschaft>, last checked 11/09/2009

Beyleveld, D., Townend, D., Rouillé-Mirza, S., Wright, D., 'Implementation of the Data Protection Directive in relation to medical research in Europe,' 2004, Ashgate Publishing, Aldershot



D7.1a User Evaluation Plan

BfDI, 'Aufgaben,' 2009, online at http://www.bfdi.bund.de/cln_111/DE/Dienststelle/Aufgaben/Aufgaben_node.html, last checked 09/09/2009

BfDI, 'Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, stellt sich vor,' 2009, online at http://www.bfdi.bund.de/cln_111/DE/Dienststelle/Bfd/BfD_node.html, last checked 09/09/2009

BfDI, 'Referat VIII,' 2009, online at http://www.bfdi.bund.de/cln_111/SharedDocs/AufgabenOrganigramm/Referat%20VIII.html?nn=408940, last checked 09/09/2009

BfDI, Tätigkeitsbericht zum Datenschutz für die Jahre 2007 und 2008, 21st April 2009, online at http://www.bfdi.bund.de/cae/servlet/contentblob/567076/publicationFile/31926/22TB_2007_2008.pdf, last checked 15/09/2009

BfDI, 'Annual Activity Report 2005/2006,' 2006, online at <http://www.bfdi.bund.de/cae/servlet/contentblob/416924/publicationFile/24940/2005-2006.pdf>, last checked 14/-09/2009

BfDI, 'Annual Activity Report 2003/2004,' 2004, online at http://www.bfdi.bund.de/cae/servlet/contentblob/416922/publicationFile/24942/AnnualReport2003_2004OfTheFederalCommissionerForDataProtection-Excerpt.pdf, last checked 14/-09/2009

"Biometric ID Cards Survey," 2009 online at <http://www.idcardsurvey.com/>, last checked 11/07/2009
Bohm, N., 'The Phorm "Webwise" System – A Legal Analysis,' 23rd April 2008, online at <http://www.fipr.org/080423phormlegal.pdf>, last checked 28/04/2009

Born, S., 'Legal Texts; Federal data protection Act,' Goethe-Institut Inter Nationes, 2001, online at <http://www.goethe.de/in/d/frames/presse/gesetzestexte/e/datenschutz-einl-e.html>, last checked 6/09/2009

Bundesrat, 'Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes,' 6th March 2009, online at http://www.bundesrat.de/cln_090/nn_8336/SharedDocs/Drucksachen/2009/0001-0100/62-09_28B_29.templateId=raw.property=publicationFile.pdf/62-09%28B%29.pdf, last checked 15/09/2009

Clayton, R., 'The Phorm "Webwise" System,' 18th May 2008, online at <http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf>, last checked 28/04/2009

Crown Prosecution Service, 'The Criminal Justice System' 2009, online at <http://www.cps.gov.uk/about/cjs.html>, last checked 05/07/2009

Copyright © 2009 by the PICOS consortium - All rights reserved.

The PICOS project receives research funding from the Community's Seventh Framework Programme.



D7.1a User Evaluation Plan

Crown, The, 'Explanatory Notes to Regulation of Investigatory Powers Act,' 2000, online at http://www.opsi.gov.uk/ACTS/acts2000/en/ukpgaen_20000023_en_1, last checked 11/07/2009

De Quetteville, 'Germany outraged by data theft scandal,' *The Telegraph*, 20th August 2008, online at <http://www.telegraph.co.uk/news/worldnews/europe/germany/2591783/Germany-outraged-by-data-theft-scandal.html>, last checked 09/09/2009

Department for Business Innovation and Skills, 'What are the BS 7799 and the ISO 27000 standards,' 2009 online at <http://www.berr.gov.uk/whatwedo/sectors/infosec/infosecadvice/legislationpolicystandards/securitystandards/isoiec27002/page33370.html>, last checked 23/08/2009

Deutsch Forschungsgemeinschaft, 'Proposals for Safeguarding Good Scientific Practice,' January 1998, Deutsch Forschungsgemeinschaft, online at http://www.dfg.de/aktuelles_presse/reden_stellungnahmen/download/self_regulation_98.pdf, last checked 15/09/2009

Deutsch Gesellschaft für Soziologie, 'Ethik-Kodex,' Deutsch Gesellschaft für Soziologie, online at <http://www.soziologie.de/index.php?id=19>, last checked 15/09/2009

DW staff, 'Telekom Hit by Widening German Data trade Scandal,' *Deutsche-Welle*, 19th August 2008, online at <http://www.dw-world.de/dw/article/0,,3576869,00.html>, last checked 09/09/2009

Europa Press Releases Rapid, 'Telecoms: Commission launches case against UK over privacy and personal data protection,' 14th April 2009, online at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570>, last checked 11/07/2009

'Europe claims UK botched one third of Data Protection Directive,' *OUT-LAW News*, 17/09/2007, online at <http://www.out-law.com/page-8472>, last checked 7/07/2009

European Commission, "Progress Report on the Single European Electronic Communications Market 2008 (14th Report)," 24th March 2009, online at http://ec.europa.eu/information_society/policy/ecommlibrary/communications_reports/annualreports/14th/index_en.htm, last checked 06/09/2009

Facebook, 'How does Beacon work?' 2009, online at <https://www.facebook.com/beacon/faq.php>, last checked 21/08/2009

Google, 'Google Latitude,' 2009, online at <http://www.google.com/mobile/products/latitude.html#p=default>, last checked 23/08/2009

Handel, 'Metro-Gruppe setzt auf RFID-Chips,' *sueddeutsche.de*, 23rd February 2005, online at <http://www.sueddeutsche.de/computer/662/321531/text/>, last checked 14/09/2009

Hanff, A., 'A Critical Evaluation of the 2006/2007 trials of Phorm Inc. Technology by BT PLC,' 4th April 2009, online at https://nodpi.org/documents/phorm_paper.pdf, last checked 10/07/2009

Copyright © 2009 by the PICOS consortium - All rights reserved.

The PICOS project receives research funding from the Community's Seventh Framework Programme.



D7.1a User Evaluation Plan

Home Office, '*Targeted online advertising: interception of communications or not, if it is, is it lawful intervention?*' 11 March 2008, online at <http://cryptome.org/ho-phorm.htm>, last checked, 09/07/2009

'House of Lords ends Durant's data protection saga,' *OUT-LAW News*, 30/11/2005, online at <http://www.out-law.com/page-6405>, last checked 7/07/2009

Information Commissioner's Office, '*Appendix 1 PIA screening process*,' 2009, online at http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/3-app1.html, last checked 24/08/2009

Information Commissioner's Office, '*Enforcement*,' 2009 online at http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx, last checked 04/07/2009

Information Commissioner's Office, '*Online notification form*,' 2009 online at <https://forms.informationcommissioner.gov.uk/cgi-bin/dprproc?page=7.html>, last checked 09/07/2009

Information Commissioner's Office, '*Who are we*,' 2009 online at http://www.ico.gov.uk/about_us/who_we_are.aspx, last checked 04/07/2009

Information Commissioner's Office, '*Your legal obligations*,' 2009 online at http://www.ico.gov.uk/about_us/who_we_are.aspx, last checked 04/07/2009

Information Commissioner's Office, '*Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003*,' 8th October 2008, online at http://www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/guidance_part_1_for_marketers_v3.1_081007.pdf, last checked 24/08/2009

Information Commissioner's Office, '*Data Protection Good Practice Note Collecting personal information using websites*,' 5th June 2007, online at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf, last checked 11/07/2009

Information Commissioner's Office, '*Data Protection Technical Guidance Determining what is personal data*,' 21st August 2007, online at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf, last checked 28/04/2009

Information Commissioner's Office, '*Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003 Part 2: Security, confidentiality, traffic and location data, itemised billing, CLI and directories*' 30th November 2006, online at http://www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/pecr_guidance_part2_1206.pdf, last checked 23/08/2009

Information Commissioner's Office, '*Scottish National Party (SNP) found in breach of privacy regulations*,' 22nd May 2006, online at http://www.ico.gov.uk/upload/documents/pressreleases/2006/snp_decision_found_in_breach_of_privacy_regulations_v2.pdf, last checked 24/08/2009

Copyright © 2009 by the PICOS consortium - All rights reserved.

The PICOS project receives research funding from the Community's Seventh Framework Programme.



D7.1a User Evaluation Plan

Information Commissioner's Office, 'The 'Durant' Case and its impact on the interpretation of the Data Protection Act 1998' 27th February 2006, online at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf, last checked 7/07/2009

Information Commissioner's Office, 'Data Protection Act Legal Guidance' 2001, online at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf, last checked 9/07/2009

International Organisation for Standardisation, 'ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk,' 2008, International Organisation for Standardisation, can be purchased online at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107, last checked 22/08/2009

International Organisation for Standardisation, 'ISO/IEC 27002:2005 Code of Practice for Information Security Management,' 2005, [International Organisation for Standardisation](http://www.iso.org), can be purchased online at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297, last checked 22/08/2009

Information Tribunal, 'Information Tribunal,' 2009, online at <http://www.informationtribunal.gov.uk/index.htm>, last checked 04/07/2009

Johnson, B., 'Outrage as new Phorm trial begins,' *The Guardian*, 30th September 2008, online at <http://www.guardian.co.uk/technology/2008/sep/30/phorm.new>, last checked 21/08/2009

Jtw, 'Deutsche Telekom Spying Scandal: Emerging Details Indicate Executives Knew More and Earlier,' *Spiegel Online International*, 18th May 2009, online at <http://www.spiegel.de/international/business/0,1518,625435,00.html>, last checked 10/09/2009

Kbs, 'Reform of the German "List Privilege" - Tiger or Paper Tiger?' *Datonomy*, 19th August 2009, online at <http://datonomy.blogspot.com/2009/08/reform-of-german-list-privilege-tiger.html>, last checked 12/09/2009

Korff, D., 'Report on the findings of the EC Study on Implementation of Data Protection Directive,' July-September 2002, available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667, last checked 09/07/2009

Kremer, S., 'München: IP-adressen dürfen von website-betrieben gespeichert werden (volltext),' *Rechtsprechung und Anmerkungen zu IT/IP*, 25 October 2008, online at <http://www.kremer-legal.com/2008/10/07/ag-munchen-ip-adressen-duerfen-von-website-betreibern-gespeichert-werden-volltext/>, last checked 09/09/2009

Kreml, S., 'Bürgerrechtler rufen zur Großdemo gegen Überwachung nach Berlin,' *heise online*, 28th July 2008, online at <http://www.heise.de/newsticker/Buergerrechtler-rufen-zur-Grossdemo-gegen-Ueberwachung-nach-Berlin--/meldung/113413>, last checked 15/09/2009

Copyright © 2009 by the PICOS consortium - All rights reserved.

The PICOS project receives research funding from the Community's Seventh Framework Programme.



D7.1a User Evaluation Plan

- Kuner, C., 'European Data Privacy Law and Online Business,' 2003, Oxford University Press, Oxford
- Leyendecker, H., und Ott, K., 'Ex-Minister Baum soll aufklären,' *Sueddeutsche.de*, 6th February 2009, online at <http://www.sueddeutsche.de/wirtschaft/859/457519/text/>, last checked 11/09/2009
- Lill, V., 'Im Visier der Lidl-Spitzel,' *Der Spiegel Online*, 29th March 2008, online at www.spiegel.de/wirtschaft/0,1518,543930,00.html, last checked 06/09/2009
- Lorber, S., 'Data Protection and Subject Access Requests,' *Industrial Law Journal*, June 2004, p. 179
- McCullagh, D., 'NebuAd grilled over hot coals in Congress over privacy,' *Cnet News*, July 17 2008, online at http://news.cnet.com/8301-13578_3-9993554-38.html, last checked 11/07/2009
- Metz, C., 'NebuAd knock's at death's door,' *The Register*, 19th May 2009, online at http://www.theregister.co.uk/2009/05/19/nebuad_shutting_down/, last checked 11/07/2009
- Metz, C., 'Phorm secretly tracked Americans too,' *The Register*, 13th August 2008, online at http://www.theregister.co.uk/2008/08/13/phorm_us_tests/, last checked 06/07/2009
- Moore, T., 'Deutsche Bahn shaken by spying scandal,' *BBC News*, 13th February, 2009, online at <http://news.bbc.co.uk/1/hi/business/7887017.stm>, last checked 09/09/2009
- MoveOn.org, 'Recent Success Stories,' *MoveOn.org*, 2008, online at http://www.moveon.org/success_stories.html, last checked 11/07/2009
- Nakashima, E., 'Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy,' *The Washington Post*, 30th November 2007, online at http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112902503_pf.html, last checked 11/07/2009
- Nodpi.org, 'FAQ,' *NoDPI*, 2009, online <https://nodpi.org/faq/>, last checked 06/07/2009
- Nodpi.org, 'Welcome To NoDPI,' *NoDPI*, 2009, online at <https://nodpi.org/>, last checked 11/07/2009
- Oates, J., 'Phorm confirms TalkTalk fail,' *The Register*, 8th July 2009, online at http://www.theregister.co.uk/2009/07/08/phorm_talktalk_terminated_confirmed/
- Oellers, C., Wegner, E., 'Does Germany Need a (New) Research Ethics for the Social Sciences,' Working Paper No. 86, June 2009, German Council for Social and Economic Data (RatSWD), online at <http://ssrn.com/abstract=1452631>, last checked 15/09/2009
- Paladine, 'NebuAd pull a fast one!' *NoDPI*, 19th May 2009, online at <https://nodpi.org/2009/05/19/nebuad-pull-a-fast-one/>, last checked 11/07/2009
- Paladine, 'Off to Brussels,' 26th May 2009, online at <https://nodpi.org/2009/05/26/off-to-brussels/>, last checked 04/07/2009



D7.1a User Evaluation Plan

Paladine, 'ICO admit BT 2007 Trials breached PECR 2003 but refuse to act!' *NoDPI*, May 31st 2008, online at <https://nodpi.org/2008/05/31/ico-admit-bt-2007-trials-breached-pecr-2003-buyt-refuse-to-act/>, last checked 24/08/2009

Phorm, 'Behind the scenes – how Webwise Discover technology works,' online at <http://webwise.phorm.com/discover/behind-the-scenes.html>, last checked 6/7/2009

Privacy International, 'Privacy international identifies major security flaw in Google's global phone tracking system,' 5th February 2009, online at <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-563567>, last checked 23/08/2009

Ram, V., 'Spying troubles for Deutsche Bank,' *Forbes*, 21st July 2009, online at <http://www.forbesing.com/2009/07/21/deutsche-bank-spying-markets-equity-banks.html?partner=contextstory>, last checked 10/09/2009

Schroeder, S., 'In Germany, Google Will Erase Street View Data on Request,' *Mashable*, 18th June 2009, online at <http://mashable.com/2009/06/18/germany-google-street-view/>, last checked 15/09/2009

Schulzki, C., Gläserne Autofahrer für Versicherungen und Fahrzeughalte, ' 13th April 2006, BfDI, online at http://www.bfdi.bund.de/cln_030/nn_531474/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/2006/VDIInterviewGlaesernerAutofahrer.html_nnn=true, last checked 15/09/2009

Schweinoch, M., Ed., 'Amendments to the German Federal Data Protection Act Special Issue 17 July 2009,' *IT Ticker*, 17th July 2009, SKW Schwarz Rechtsanwälte Steuerberater Wirtschaftsprüfer Partnerschaft, online at www.skwschwarz.de/index.php?article_id=177&filename=it-ticker_sonderausgabe_bds_g_englisch_2009-07-18_1.pdf, last checked 12/09/2009

Siegismund, E., 'The Public Prosecution Office in Germany: Legal Status, Functions and Organization,' *UNAFEI Annual Report for 2001 and Resource Material Series No. 60*, pp.58-76, February 2003, online at <http://www.ncjrs.gov/App/Publications/abstract.aspx?ID=201695>, last checked 11/09/2009

Stoppt die Vorratdatenspeicherung, 'Verwaltungsgericht: Vorratsdatenspeicherung ist "ungültig,"' 16th March 2009, online at <http://www.vorratsdatenspeicherung.de/content/view/301/1/lang.de/>, last checked 15/09/2009

Telegraph Staff, 'Phorm raises £15m to expand targeted online advertising service,' *The Telegraph*, 10 June 2009, online at <http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/5492922/Phorm-raises-15m-to-expand-targeted-online-advertising-service.html>, last checked 06/07/2009

UK Police Portal Team, 'UK Forces List,' 2009, online at www.police.uk/forces.htm, last checked 06/09/2009

Copyright © 2009 by the PICOS consortium - All rights reserved.

The PICOS project receives research funding from the Community's Seventh Framework Programme.



D7.1a User Evaluation Plan

Ulbricht, C., 'Is it legal to use Google Analytics - Data protection in Germany,' 14th November 2008, online at <http://www.german-weblaw.com/index.php?/archives/3-Is-it-legal-to-use-Google-Analytics-Data-protection-in-Germany.html>, last checked 15/09/2009

Waters, D., 'Phorm – one year on,' *BBC News*, 4th March 2009, online at http://www.bbc.co.uk/blogs/technology/2009/03/phorm_one_year_on.html, last checked 21/08/2009

Waters, D., 'Home Office Colluded with Phorm,' *BBC News*, 2009, online at <http://news.bbc.co.uk/2/hi/technology/8021661.stm>, last checked 28/4/2009

Web Team, 'Google Latitude,' *The Freedom Bill*, 17th March 2009, online at <http://freedom.libdems.org.uk/google-latitude/>, last checked 23/08/2009

Williams, C., 'Jacqui calls Vodafone man to run massive snoop database,' *The Register*, 18th December 2008, online at http://www.theregister.co.uk/2008/12/18/imp_tim_hayward/, last checked 11/07/2009

Working Party 11, Eds., Cuijpers, C., Roosendaal A.,

Koops, B., "D11.5: The legal framework for location-based services in Europe," 12 June 2007

Wray, R., 'Phorm plunges as BT mothballs targeted ads service,' *The Guardian*, 6th July 2009, online at <http://www.guardian.co.uk/business/2009/jul/06/phorm-webwise-bt-internet-privacy>, last checked 6/07/2009

Wray, R., 'http://www.guardian.co.uk/business/2009/jul/07/carphone-warehouse-talktalk-drops-phorm' *The Guardian*, 7th July 2009, online at <http://www.guardian.co.uk/business/2009/jul/06/phorm-webwise-bt-internet-privacy>, last checked 8/07/2009



3 Appendices

Appendix I - User Consent form

PICOS Angling Community Prototype Testing User Consent form

Legal notice and consent form, including specific information, consent and agreement form for the PICOS Angling Community

This legal notice is to be submitted to the individual volunteers, who are interested in participating in the PICOS (Privacy and Identity Management for Community Services) Angling Community Prototype Lab Tests and Field Trials, before the start of the lab tests and the field trials and shall be collected by the PICOS partner, CURE (represented by Ms Eva Ganglbauer, Hauffgasse 3-5, 1110 Vienna, Austria).

Information about the PICOS Angling Community Prototype Lab Tests and Field Trials and the processing of your personal data, including location data

You, a volunteering individual, are hereby informed of the details of the PICOS Angling Community Prototype Lab Tests via questionnaires and the PICOS Angling Community Prototype Field Trials via a Nokia 5800 XpressMusic mobile device. You are fully free to participate in the test or not. *Only* in case you agree with the information and the consent drafted below, you are invited to sign and date this form for consent and agreement and to return it to CURE.

About the PICOS Angling Community Prototype.

The PICOS Angling Community Prototype (hereafter “the Prototype”) has been developed by the PICOS Consortium, which is a European funded (FP7) research project (Grant Agreement 215056). The PICOS Angling Community Prototype is an identity management system with enhanced trust and privacy functionalities.

About the responsible for the organization of the PICOS Angling Community Prototype Lab Tests and Field Trials.

Ms Eva Ganglbauer, as representative of CURE (Hauffgasse 3-5, 1110 Vienna, Austria), which is a PICOS partner, is the responsible for the organization of the PICOS Angling Community Prototype Lab Tests and Field Trials. You can have access to your personal data



and ask for their correction by contacting Ms Eva Ganglbauer at ganglbauer@cure.at, tel: +43.1.743 54 51.42 or fax: +43.1.743 54 51.30.

About the purposes for which your data will be processed.

Your data that will be collected during the PICOS Angling Community Prototype Field Trials via a Nokia 5800 XpressMusic mobile device, as well as the data that will be collected during the PICOS Angling Community Prototype Lab Tests via questionnaires are going to be processed for scientific research purpose and in particular (i) the testing of the proper functioning of the PICOS Angling Community Prototype, which is developed within the PICOS project, (ii) the testing of the mechanisms developed in the PICOS Angling Community Prototype, (iii) the assessment of the interaction between the users and the application, and (iv) for getting user feedback (by questionnaires and interviews). Your data will not be used for any further purposes beyond the above mentioned and will be deleted when the research purpose is completed and at the latest by the end of the PICOS project, i.e. 31.01.2011.

About the data that will be processed.

A login name and a password are needed for registration and will be used for further authentication, although no real data, e.g. name, phone, e-mail address are required during registration. You will communicate in the Angling community via pseudonym (= partial Identities) chosen by you at registration or later. Any further information relating to your gender, age, address, e-mail, mobile phone number, hobbies, personal preferences, as well as your location and status of presence⁴²⁷ will be freely provided by you and only if you wish for (optional data).

In order to minimize the data, you do not need to mention your name or any reference number on the questionnaire.

The full privacy policy of the PICOS Angling Community Prototype, which is not clickable in your mobile device, can be found as an Annex to this document.

About your location data.

Hereby you consent to the processing of your location information, when you decide to do so via the PICOS enabled mobile phone. Your full location data may be accessed from your mobile handset, and sent to the PICOS platform. However by default this functionality is turned OFF. **By turning ON the switch, you consent to your location data being disclosed.** This functionality must also be enabled in the general location policy and must be expressly "allowed" in order for the location data to be sent to the selected sub communities, a contact

⁴²⁷ The following types of information can be optionally disclosed via the PICOS Angling Community Prototype: e-mail, gender, age (interval), zip-code, country, mobile phone number, avatar (any image), favourite fishing methods, favourite target species, favourite watercourses, fishing since xx years, membership clubs, number of contributions visible, reputation level, instant messaging name (e.g Skype), hobbies, favourite fishing destinations, presence, location, preferred contact means.



or to the whole public community. You, the user, are also able to specify the level of blurring in the partial identity (1 km, 5 km, no blurring), which is a global setting and effects all your identities.

About recording videos and taking photos during the lab and field tests.

During the lab and field tests, videos will be recorded and photos be taken to document the tests. The data will be dealt with in a confidential and anonymous way and will only be used for research purposes, as described above. Moreover, the recorded data will only be used for evaluation and review and will not be made public.

Security measures.

Appropriate security policies, rules and technical measures are implemented to protect your personal data that will be revealed via the Prototype and will be stored on the PICOS Platform from unauthorised access, including use of firewalls where appropriate.

All the employees and data processors, who have access to, and are associated with the processing of personal data, are obliged to respect the confidentiality of the users' personal data.

We ensure that your personal data will not be disclosed to State institutions and authorities except if required by law or other regulation.

About your use of the Nokia 5800 XpressMusic mobile device.

If you are interested and willing to participate in the testing of the PICOS Angling Community Prototype, you will receive a Nokia 5800 XpressMusic mobile device, which will be returned to CURE upon the end of the field trial. If you fail to return the mobile device, you shall pay a fine of 230 EUR.

About the host of the PICOS server.

The participating PICOS partner being operator of the PICOS servers, Hewlett-Packard Centre de Compétences France (Avenue Raymond Chanas 5 – 38053 Grenoble, France) will be a processor in the field test, as it hosts the PICOS Servers in their premises at Hewlett-Packard Centre de Compétences France, and will process information on behalf and upon further instructions of CURE.

About the questionnaires relating to the PICOS Angling Community Prototype.

CURE will invite participants in the PICOS Angling Community Prototype to complete a questionnaire and to participate in interviews and video analysis. Any and all information collected by CURE through the evaluation methods distributed amongst the participants in the PICOS Angling Community Prototype will be on a no name basis and the information provided should in principle not be linkable to a particular user.

Free, Specific, and Informed consent.

Copyright © 2009 by the PICOS consortium - All rights reserved.

The PICOS project receives research funding from the Community's Seventh Framework Programme.



D7.1a User Evaluation Plan

I understand and agree by signing below that the above described categories of personal data, in particular (i) login name, password and pseudonym(s) (ii) data relating to my gender, age, address, e-mail, mobile phone number, hobbies, personal preferences⁴²⁸ and (iii) data relating to my location and status of presence, (iv) pictures and video shooting, (v) completed written answers to the questionnaire sent to CURE, will be processed by CURE, the data controller, represented by Ms Eva Ganglbauer, with registered address in Austria, Hauffgasse 3-5, 1110 Vienna, solely for test and scientific research purposes, in particular for the testing of the proper functioning of the PICOS Angling Community Prototype, which is developed within the PICOS project, and the evaluation of ergonomics and acceptance of the test users. These personal data, including the traffic and location data, will only be processed for the duration of the PICOS Angling Community Prototype field trials and lab tests and the analysis of the data in the framework of the PICOS project, and will be deleted upon the end of these tasks and definitely by the end of the PICOS project, i.e. the 31st of January 2011.

The representative of CURE in Germany, is the Leibniz Institute of Marine Sciences at the University of Kiel (IFM-GEOMAR), Department of Fisheries Biology, Duesternbrooker Weg 20, D-24105 Kiel, Germany (Contact person: Bernd Ueberschär, at bueberschaer@ifm-geomar.de).

The participating PICOS partner being operator of the PICOS servers, Hewlett-Packard Centre de Compétences France, Avenue Raymond Chanas 5 – 38053 Grenoble, France, will be a processor in the field trials, as it hosts the PICOS Servers in their premises at Hewlett-Packard Centre de Compétences France and will process that data only on behalf and according to the instructions of CURE.

I am informed and take note that I have access to my personal data and the right of correction. For such purpose, I can contact the representative of CURE in Germany, IFM GEOMAR, and its contact person Bernd Ueberschär at bueberschaer@ifm-geomar.de, tel: +49 431 600 4572 or fax: +49 431 600 1515; or if I would prefer, CURE represented by Ms Eva Ganglbauer at ganglbauer@cure.at, tel: +43.1.743 54 51.42 or fax: +43.1.743 54 51.30. I can also delete at all times my data from the Prototype. After the end of the field test, I agree to return the NOKIA 5800 XpressMusic mobile device, given to me for the purposes of the field trial, or else I agree to pay a fine of 230 EUR.

In using the PICOS Angling Community Prototype I understand that data are transmitted via a mobile operator. The processing of traffic and location data, as well as any other data collected by this operator, fall outside the control of CURE and solely these mobile operator is responsible for the processing of these data and for which they become controller.

For consent and approval:

⁴²⁸ The following types of information can be optionally disclosed via the PICOS Angling Community Prototype: e-mail, gender, age (interval), zip-code, country, mobile phone number, avatar (any image), favourite fishing methods, favourite target species, favourite watercourses, fishing since xx years, membership clubs, number of contributions visible, reputation level, instant messaging name (e.g Skype), hobbies, favourite fishing destinations, presence, location, preferred contact means.



D7.1a User Evaluation Plan

Date Name Signature

Optional:

In case you agree that videos and photos of you are used for dissemination of the PICOS Project and made public (e.g. at conferences, papers, workshops, etc) please check the box below:

I agree that videos and photos where my person is visible are made public for dissemination of Picos results. The public photos and videos will not contain meta-information including my name.

Date Name Signature

Annex:

The Privacy Policy of the PICOS Angling Community Prototype



Appendix II - Picos Privacy Policy

Tuesday, October 28, 2009

PICOS Angling Community Privacy Policy

This privacy policy governs your PICOS Angling Community account and any information you provide to the PICOS partner, the Center for Usability Research & Engineering (CURE), in relation to the use of the PICOS Angling Community Prototype. **By accepting the PICOS Angling Community Privacy Policy (hereafter Privacy Policy), you expressly consent to the use of your personal information as indicated in this Privacy Policy.**

The service provided by the PICOS consortium is for scientific research purposes, in particular the testing of the proper functioning of the PICOS Angling Community Prototype, which is developed within the PICOS project, and for testing the mechanisms developed in the PICOS Angling Community Prototype and assessing the interaction between the users and the application. Any processing of personal data is to achieve these principal aims.

This privacy policy covers the PICOS consortium and its Angling Community Prototype.

The data controller for this service is:

Organisation name: Center for Usability Research & Engineering (CURE)
Address: CURE, Hauffgasse 3-5, 1110 Vienna, Austria
Controller: Johann Schrammel, on behalf of CURE
Telephone: +43.1.743 54 51.18
Fax: +43.1.743 54 51.30
Email: schrammel@cure.at

The PICOS consortium takes your privacy very seriously and as such, we undertake to use your information only in accordance with the terms of this privacy policy.

Data collection and Purpose Specification

We only collect data for the principal aim of providing you with a privacy-friendly social networking experience of the PICOS Angling Community Prototype for research purposes.

We undertake not to sell, or otherwise disclose, or share your personal identifiable information to third parties without your expressly given consent. We further undertake to only collect personal data that you volunteer to us. We do not collect data from other sources, such as public records or bodies, or private organisations.

Copyright © 2009 by the PICOS consortium - All rights reserved.

The PICOS project receives research funding from the Community's Seventh Framework Programme.



The data we collect about you can be accessed at any time via the PICOS Angling Community Prototype installed on your mobile device and may be amended, or revoked at the request of the user at any time.

Confidentiality and Security

We have implemented appropriate security policies, rules and technical measures to protect the personal data that we have under our control from unauthorised access, including use of firewalls where appropriate.

All our employees and data processors, who have access to, and are associated with the processing of personal data, are obliged to respect the confidentiality of the users' personal data.

We ensure that your personal data will not be disclosed to State institutions and authorities except if required by law or other regulation.

Access to the personal data we may hold about you

All personal data stored concerning yourself may be accessed directly via the PICOS Angling Community Prototype installed on your mobile device and may be deleted or revoked or amended directly by you, the user.

We do not reserve the right to refuse to provide you with a copy of your personal data.

Privacy compliance

This privacy policy, and our use of your personal data, is compliant with the Austrian legislation. Specifically we undertake to adhere to the principles of 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, as implemented into the Austrian legislation in the Austrian Data Protection Act (Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000), BGBl. I Nr. 165/1999, idF. BGBl. I Nr. 136/2001 of 17.08.1999) and any other relevant provision of the Austrian legislation, where applicable.

Personal data collected and instances of disclosure.

Only the following three types of information are mandatory upon registration: Real name, pseudonym and password. All additional data collected is principally optional however it is partially necessary if the user wants to facilitate internal communication with other members.

The purpose of PICOS is about the sharing of information in a privacy-friendly manner. Therefore you, the user, controls what type of information is collected and disclosed with the creation of partial identities. Only this selected information will be disclosed to other members of the community.



D7.1a User Evaluation Plan

With the creation of a new partial identity, the user decides what personal data shall be shown in combination with this partial identity. The user has the choice to select in a fine-grained manner what kind of personal data should be visible for each single purpose/service.

In the case of deletion of a user profile, no data is retained except for contributions in the form of posts to forums.

Your full location data may be accessed from your mobile handset, and sent to the PICOS platform however by default this functionality is turned OFF. **By turning ON the switch you consent to your location data being disclosed.** This functionality must also be enabled in the general location policy and must be expressly “allowed” in order for the location data to be sent to the selected sub communities, a contact or to the whole public community. You, the user, are also able to specify the level of blurring in the partial identity (1 km, 5 km, no blurring), which is a global setting and affects all your identities.

By accepting this privacy policy, you agree your “presence” data (i.e. whether you are online, absent, busy) is sent to the PICOS platform. Other users are informed of your presence only after you have expressly consented to this disclosure.

Deletion of data

Your data will be deleted when the purpose for which the data are processed is completed, i.e. when the testing of the proper functioning of the PICOS Angling Community Prototype, which is developed within the PICOS project, and the testing of the mechanisms developed in the PICOS Angling Community Prototype and the assessment of the interaction between the users and the application are completed. At the latest by the end of the PICOS project, i.e. 31.01.2011.

Use of data for statistical purposes

Access data may be collected anonymously for statistical reasons.