Human Brain Project

# Citizen's view on data protections and privacy in research projects BULGARIA

*Compiled by*: Zoya Damianova

**March 18, 2016**

**Contact details for corresponding author:**
Zoya Damianova
zoya.damianova@online.bg

This report is part of the project
*The Human Brain Project (HBP), sub-project 12 'Ethics and Society'*- which received funding from the European Commission's Seventh Framework Programme *(FP7/2007-2013)* under grant agreement n° *604102 (HBP)*

European Commission

**Contents**

## EXECUTIVE SUMMARY

This report presents the results from a citizen consultation within the Human Brain Project, held in Bulgaria, on February 13th 2016. A total of 30 citizens came together to discuss issues of privacy and personal data protection in scientific research. They worked at three different tables of 10 participants each, and had to come up with questions on personal data protection, privacy issues, and the use of personal data for research. Each question was answered at two of the tables by different participants, thus providing a rich data set of opinions.

The Bulgarian citizens elaborated 16 raw problems they thought still existed with regards to personal data protection. By merging similar problem statements and further analysis, the 16 raw problem statements were reduced down to 10, thus also allowing cross-table comparison. This provided further insight into the most pressing issues for the participants.

The report provides a brief overview of key indicators on Bulgaria. In section 2, it provides an overview of participants' demographic profile, and of the responses to a questionnaire that was handed to them following the start of the event. Section 3 provides the overview of all group interview sessions. In section 4 the report details the most pressing problems and the recommendations provided by the citizens for each identified problem.

# 1 INTRODUCTION

In February 2016, the Human Brain Project (HBP) hosted citizen meetings in Austria, Bulgaria, Poland, Portugal, the Netherlands and Sweden. The HBP citizen meetings were set up to provide the public with an opportunity to reflect on issues related to privacy and data protection in research projects, and to provide their ideas and opinions directly to the researchers and managers of the HBP. The present report is one of 6 country reports detailing the result of the national meetings. The results of all six citizen meetings will be collected in a main report and delivered to the researchers and managers of the HBP project. The reports will also be made publically available.

The report first gives a brief overview of the context of Bulgaria, before proceeding to the results.

*[Methodology will be explained in the main report]*

## 1.1 BULGARIA

The aim of this report is to analyze citizens' perception of data protection and privacy issues in research projects. The goal is to provide HBP researchers and management with input they can use to plan the design of data collection and processing procedures in the HBP. We will begin with providing some basic information about Bulgaria.

Bulgaria has a total population of around 7,36 million people, per the last census data from 2011, but its population is declining on a year-to-year basis (by 2030, it is expected to dwindle to 6,5 million[1]). The population is predominantly Bulgarian (84,8%), with the most sizeable minorities being the Turks (8,8%) and the Roma (4,9%)[2] spread unevenly across the different regions.

The GDP has been growing slowly since the economic crisis of 2008-2009 and for 2015 is around 42 bln EUR (3% growth rate), or slightly more than 5,800 EUR per capita. Despite the positive, albeit slow, economic development and the generally good macroeconomic situation, the average monthly salary remains at the lowest levels in the EU at just 452 EUR in 2015[3], and Bulgaria is still among the poorest EU Member States.

[1] Source: National Statistical Institute, http://www.nsi.bg.
[2] Source: National Statistical Institute, Census 2011. Data available at http://www.nsi.bg/census2011/pagebg2.php?p2=175&sp2=190.
[3] Sources: Wikipedia, https://en.wikipedia.org/wiki/Bulgaria; National Statistical Institute, http://www.nsi.bg.

Since 1989 Bulgaria has been a parliamentary democracy. The National Assembly consists of 240 seats, and is elected in popular elections for a term of 4 years. The Parliament nominates a Prime-Minister and approves the structure and proposed members of the Coucil of Ministers. The figure of the Prime Minister is the most powerful in the executive branch. Also part of the executive power, though with limited responsibilities, is the President, elected in popular elections for a term of 5 years. Every four years, local elections are held for Mayors and City Councils in each of the 265 municipalities of the country.

R&D spending in Bulgaria has remained low compared to the EU average. Until 2008, it has mostly stayed around 0,48% of GDP, even though actual spending in nominal terms had been growing. This trend was reversed in 2009 since when the share of R&D expenditure has started to grow and reached 0,78% in 2014 (latest available data) as show on Figure 1.

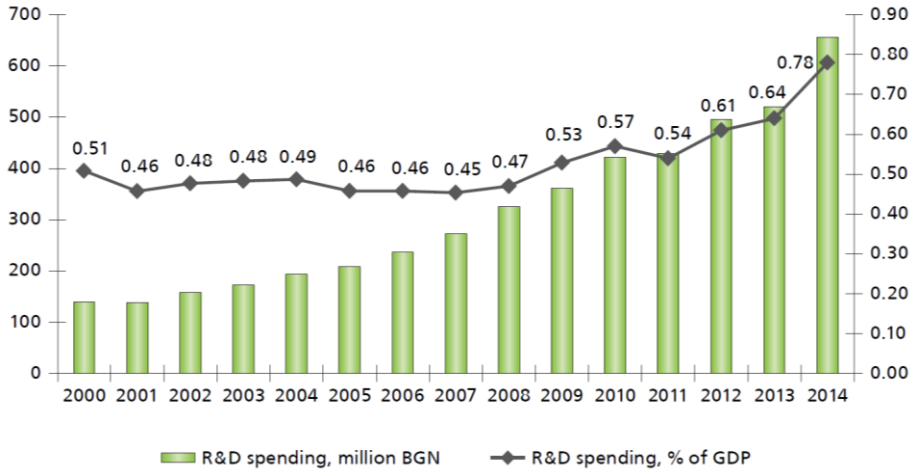


**Figure 1** R&D Spending in Bulgaria (2000-2014)[4]

That increase, especially since 2010 onwards, has been due to the increase in spending from foreign sources (such as the EU structural funds and framework programmes). According to analyses by ARC Fund, external funding is becoming critical for the existence and development of the national research and innovation system[5]. Figure 2 provides a more thorough overview of these trends.

Also growing is the amount invested in R&D by private sources, whereas those spent by the public sector have dropped significantly since 2008 and are only slighly picking up since 2012 (in absolute terms). However, as depicted by Figure 3, the share of R&D expenses of the

[4] Source: ARC Fund (2015). Innovation.bg: The Innovative Bulgarian Companies, p.45. Accessible at http://www.arcfund.net/fileSrc.php?id=22695.
[5] Ibid.

public sector is declining rapidly. The amounts invested by non-commercial organisation and by higher education institutions are negligible compared to the rest.

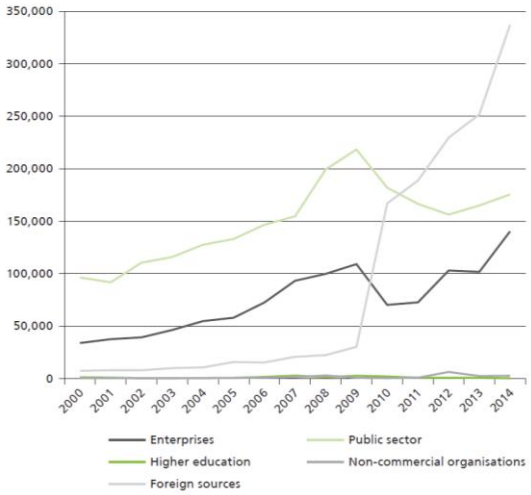


**Figure 2** R&D Spending by source (2000-2014)[6]

Figure 3 also provides a comparative picture in percentage terms for the shares of GERD investments by source, as well as the percentage of all GERD of the total GDP (depicted on the right-hand scale, and marked by the dashed line). It can be seen that the overall increase in the total GERD share is due to the foreign sources (more than 10% increase over the period 2010-2014), and to a lesser extent – to the private sector.

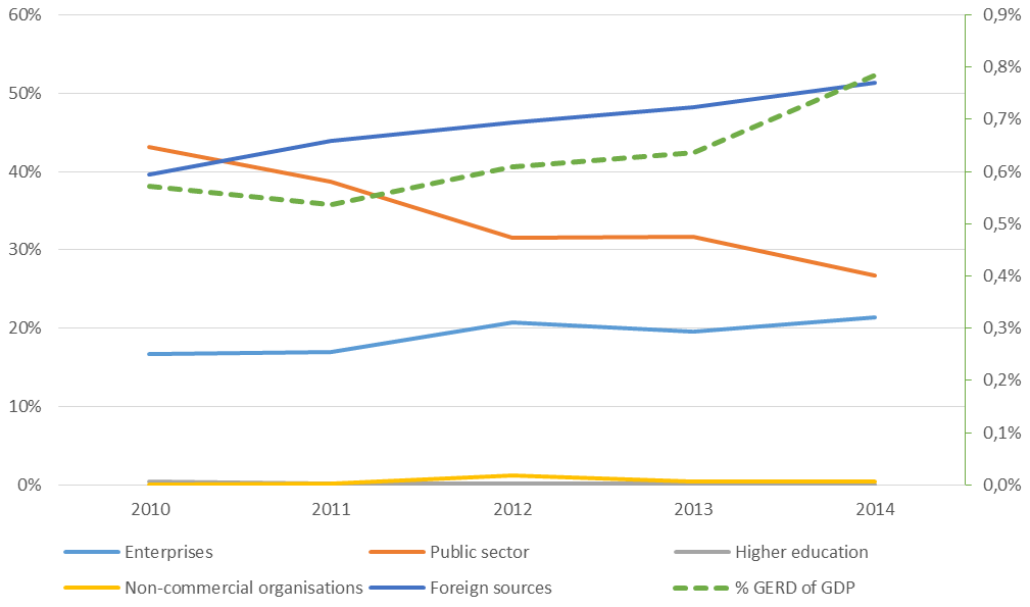


**Figure 3** GERD spending by source, and % of total GERD of total GDP[7]

[6] Source: ibid.
[7] Source: National Statistical Institute, http://www.nsi.bg.

# 2 RESULTS FROM THE QUESTIONNAIRE

All 30 participants had filled in the questionnaire. Twenty-five of them (or 83%) confirmed the questions matched well with the distributed information material, while two claimed the questions were biased. Another three respondents did not wish to respond to that question.

## 2.1 DEMOGRAPHIC PROFILE

The Bulgarian consultation took place in the city of Plovdiv, which is the second largest city in the country. A total of 30 participants attended, with the majority from the city itself, and a smaller number from the surrounding rural areas. Of them, 17 (56%) were women, and 13 (44%) men[8]. In terms of age, 13 of the participants (43%) were between 18-25 years old, 9 (30%) were between 26-40, 6 (20%) between 41-55, one participant was between 56 and 65, and one was above 65[9]. The average age of the participants was 31,9. Higher education was reported by 17 (57%) people, 12 (40%) indicated a completed high-school, and only 1 reported to have completed primary education[10]. In terms of their employment status, 18 (60%) of the participants indicated they were currently employed, 7 (23%) were students, 4 (13%) were unemployed and 1 was retired[11]. When asked about the specific sector, in which they were employed, 4 of the participants indicated *ICT*, 2 marked *Science*, 1 did not wish to answer, and 19 (more than 63%) reported "Other". Of those, 3 indicated media or journalism, 2 wrote NGO or social services, 3 were students, while others' responses included judiciary system, engineer, education, services, electrical equipment, and arts.

## 2.2 MOTIVATION TO JOIN THE HBP CITIZEN MEETING

The majority of participants (18, or 60%) indicated they had thought of the meeting as an opportunity to learn more about data protection and privacy issues in research. Six (20%) indicated they follow news on privacy and data protection, and 5 admitted they were worried about privacy and data protection. Only one participant indicated he or she liked the opportunity to have his or her voice heard in an EU research project. No one admitted to have had any issue of privacy and data protection play role in their own life.

## 2.3 THE INFORMATION MATERIAL

[8] This is based on data provided during the recruitment process. Only 22 of the participants chose to indicate their gender on the distributed questionnaire.
[9] Age figures are based on data provided during the recruitment process.
[10] Education figures are based on data provided during the recruitment process.
[11] Employment figures are based on data provided during the recruitment process.

For the large majority of participants (23, or 77%) the information booklet had given a good overview of the issues related to data protection and privacy in research. For 4 of the participants, the information provided, however, seemed biased. Two indicated the booklet was easy to understand, and one marked "Other" and further commented that the material included "unknown terminology".

### 2.4 ISSUES OF PRIVACY, DATA USE AND PROTECTION

Participants shared a largely uniform opinion about what privacy is. Nearly two thirds (19) consider privacy to refer to their ability to choose what information about them is shared with third parties. Only 4 participants (13%) referred to transparency in how information about them is being used. Two participants admitted they had no idea what privacy was, and two others indicated a preference that their employer would not be able to access their health data. Only one participant insisted on certainty their data would not be used for profit purposes by private companies.

With respect to what they considered to be personal data, responses were distributed almost uniformly across the different answer options, with the largest number of responses (8) however being about ***all*** of the listed examples – data about personal activities (4 votes), political views (4 votes), religious views (2 votes), health status (3 votes), content of correspondence (5 votes). Only 2 of the participants disagreed with all of the options and 2 more did not wish to answer.

The same proportion of participants indicated that in order for their data to be protected, they would expect it to be anonymised, but also that an Ethics Committee would review if the protection is adequate. Only 5 of the participants were content with anonymization only as a sufficient measure for protection. Three of the participants demonstrated a preference that they would be asked for informed consent every time researchers would like to use their data unless the data has already been anonymised. Only one participant did not feel a need that his or her data was protected in any way, and one chose the option "Other", commenting that it would depend on the consequence of the data used, and insisting on having given permission for the use of data, with or without the option for anonymisation.

However, when asked to think whether anonymisation is adequate protection for their personal data, only one participant answered "Yes", while 9 (30%) marked "No" and another 11 (37%) were not sure. Another 8 (27%) participants expressed a particular doubt in the level of protection provided by anonymisaiton, saying they worry about hackers breaching into

their data, or about new technological developments that would surpass the limitations imposed by anonymization. One participant did not wish to answer.

With respect to *who* can actually use personal data, there were two distinct groups of responses. Thirteen (43%) of the participants were comfortable with having only public and private organisations conduct research with their data, while another 12 (40%) indicated they did not think there should be any restriction on who has access to their data. Only 1 participant preferred that only publicly funded entities are allowed to conduct research with his or her data, another 1 was at the other extreme opinion that no one should be able to conduct research using personal data. One did not wish to answer and 2 chose the option "Other" (however responses were recorded on three of the questionnaires). One comment was that "no one should be allowed to use one's personal data without the knowledge of that person". Another was more restrictive, specifying that no personal data should be accessible, "except when concealing information needed by employers and institutions". The third comment emphasised the need for one's explicit consent in using his or her data.

When asked about how to solve the trade-off between privacy and research, nearly half of the participants (14, or 47%) indicated their privacy is more important than any research, while only 3 were at the opposite opinion. Six indicated that high level of protection is only necessary for some types of data, while only 1 stated he or she did not feel his or her data needed specific protection. Another 6 participants did not wish to answer.

Nineteen of the participants (63%) further stated that they do not feel informed enough about who has access to their data and what it is being used for, as opposed to just one person who said he or she did feel informed. Only two more people provided answers to that question, marking the option "Other". In one of the comments, the participant had noted that in Bulgaria "there is no awareness of how, where and by whom our data is used." The other comment emphasised the very low levels of trust stating that "[even though] I am aware of who has access to my personal data… I am not sure that others do not use [them]."

An overwhelming majority of the participants – 27 (90%) indicated they did not know where they could get more information about the use of their data, while only 2 provided an affirmative response. One of respondents chose the option "Other", noting further that usually the information available is still incomplete.

### 2.5 USING DATA IN RESEARCH

When it comes to worries of how data is being used for research, 14 (47%) of the participants note that they worry that their data would be used for personal or financial gain rather than for

scientific progress. A slightly smaller share of 11 people (37%) are worried about where their data will ultimately end up. One has doubts whether the outcomes of research would actually benefit society, 3 are worried that their data might be used against them, and 1 participant did not wish to answer. When asked of the consequences of sharing their data, only 8 (27%) of the respondents were certain only they would be affected, while a sizeable majority of 21 people (70%) were concerned that certain types of data may have consequences for members of their families too. One respondent did not wish to answer.

Scientists were seen as in need of specific competencies when it comes to handling data. Twelve (40%) of the participants believe scientist should have had some training in handling personal data, and another 9 (30%) expect that scientists will be able to keep one's data private. Four said they would expect scientist to inform them if they found any leads about possible illnesses, and 3 stated they would not want their data to be used for any other research that what was originally agreed to. One person did not wish to answer, and one marked the option "Other". Two people made further notes to this question. One stated that scientist should not be held responsible for the protection of personal data, as responsibility had to lie with the ones who actually administer the data in the first place. The other comment insisted on researchers' being familiar with the protection of personal data, even though that is not their primary responsibility.

With respect to research projects, participants still viewed anonymisation as a necessary precondition to have their data used. Twelve (40%) agreed to their data being used for anything researchers deem appropriate, if the data were properly anonymised. Eight people were a little stricter in saying that, if anonymised, their data can be used only for the research project they agreed for. Another six people would agree to have their data used for any type of research, as long as the data were anonymised. Only one person responded that if the data were not anonymised he or she would have to be asked for permission each time the data would be needed for a research project. This suggests that anonymisation would provide sufficient incentive for people to agree to have their data used for research.

# 3 THEMES FROM THE GROUP INTERVIEWS

## 3.1 THE MEANING OF PRIVACY

### 3.1.1 What is personal data

Participants had a relatively thorough idea of what constitutes personal data and could quickly identify examples thereof, such as - full name, telephone number, identification number, and residential address, religious and political views. One participant mentioned bank records as well, while the majority considered health-related data as personal data that is in need of high protection.

Everyone agreed that any person should be informed, or at least have the means available to inform her- or himself, of how his or her data is being accessed and used, and be clear about who is in possession of the data and how the data is being stored and protected. The participants further agreed that the proper protection of personal data will also result in the protection of meta-data.

Participants insisted that there is a pressing need for higher levels of awareness - both among citizens about how their data is being collected, processed, and stored, and among those who administer personal data. Most admitted very openly they did not know who could legally store their data, and even less so - about what happens to the data once it gets shared. Moreover, they were unaware of any possibility how to learn about this. The fact that there is a special law, as well as a special commission dealing with the protection of personal data, was largely unknown, and none of the participants knew of any details.

### 3.1.2 Reflections on consequences of misuse, who is affected/how

During the interviews, a few of the questions explicitly inquired into the risks of possessing pools of personal data and the consequences of misuse thereof. The participants agreed that any organisation/authority that stores or otherwise uses personal data should have clear and accessible ways to share information with citizens about the methods of storage and types of data uses.

The likelihood of data misuse, i.e. data being used for purposes other than that it is stored for, was rated rather high by all participants. The same attitude was demonstrated not only for a hypothetical case whereby personal data is being stolen, but also with respect to opportunities available to data administrators to obtain personal gain by sharing or otherwise exporting records away from the original storage location. Expected consequences quoted include financial loss, damaging one's reputation in the community, negative social consequences

(i.e. revealing the secret of adoption to the adopted child before his or her parents choose to do so; revealing one's HIV positive status, etc.), and negative consequences to one's family.

Furthermore, most of the participants favoured highly a specialised body tasked with prosecuting personal data abuse or misuse. There was a strong demand among participants that there is such a body where they can go and file a complaint if they feel their data is threatened by a particular data administrator. Most of the participants however were unaware that there exists a special Commission for Personal Data Protection, whose responsibilities in large part match such expectations and demands.

## 3.2 PROTECTION OF PERSONAL DATA

A lot of the participants believe that certain data have to be subject of protection as a priority. Besides typical sensitive data (i.e. health records and personal identification data, which participants referred to in their examples without calling that data "sensitive"), a few stressed out also genetic data and the data on movement and current location as being in need of higher priority protection. One participant further elaborated that any data depicting one's psychological or mental character should also be protected highly. Thus, in participants' view, more stringent data protection should be applied well beyond what constitutes personally identifiable data.

However, there is a lot of confusion when it comes to how citizens have to be informed about how (well) their data is protected. It was only during the discussions that the participants started thinking about who is in charge of protecting personal data, and whether their own personal data are being handled in a safe manner. One group of opinions suggested that a Facebook-like model be followed, i.e. it should be up to the individual to safeguard his or her own data, and only share with others - individuals or institutions - what he or she deems necessary.

### 3.2.1 Views on anonymisation

There were three distinct views on who is to be responsible for data anonymisation. Most opinions were focused on the role of scientists themselves, i.e. they are the ones who have to anonymise data before using it. For most participants, assigning such role to scientists/researchers was a mere detail. Still, a required limitation was suggested, namely that scientists should only be granted access to the data they would need for their research, but not more. Anonymisation, in this sense, at least in terms of responsibility and scope of application, would remain fairly limited. A widely shared assumption was also that scientists

would be knowledgeable (i.e. through special training) of how to anonymise data, rather than rely on external algorithms.

Another group of participants were of the exact opposite opinion, stating that anonymisation should not be left to scientists, but should instead be dealt with by "experts", different from scientists, who were believed not to possess the needed knowledge or skills in order to be handed over such responsibility. Those experts would have to work in teams, alongside, but nonetheless separate from, the scientists/researchers using the data. In effect, only those experts would deal with the original data, but they will not be able to use it for anything else.

A third opinion that partly extends on the above, is that anonymisation would best be handled by an external body, or even a special (centralised) institution. Such an institution, according to participants' opinions, might help standardise anonymisation techniques and rules, thus guaranteeing that data misuse or abuse that also leads to identifying the original subjects would not be possible for any scientist/researcher or institution.

### 3.2.2 Perspectives on consent

The notion of consent - in all of its forms - was not unequivocally understood by all participants. Most were in fact rather confused and perceived consent in mechanical terms - the act of signing a consent form was all they imagined, and were very distrustful and doubtful of its effect. Many of the participants said that often, when they are asked for their consent prior to a medical procedure, or when signing a binding contract for a service (i.e. mobile phone plan), the conditions described are well beyond the very purpose of why they need to sign the consent form. Thus, the consent form enables the ones handling the data obtained to have much looser responsibility and much greater opportunity to use the data in ways they see as appropriate.

There was clearly very low level of awareness about the currently existing rules and regulations on personal data protection. Even though there is a special Law for the Protection of Personal Data, and a State Commission for Personal Data Protection12, the majority of participants kept referring to the need for regulation and for the establishment of a dedicated state body to be responsible for any personal data protection activities. Some were even more insisting in that such a body is the ultimate monitor over all administrators of personal data that should also handle all individual complaints and impose sanctions on those entities that dared to misuse personal data, regardless of the reason. The act of consent was commented

[12] See https://www.cpdp.bg/en/index.php?p=home&aid=0.

from that perspective as becoming a tool for control over how one's data is being used since if the data were to be used for any other purpose or intention, one could then notify the specialised body. That was agreed upon as a sufficient restrictive measure.

Most notably, participants struggled with imagining scenarios when data could be legally used without prior consent, thus effectively overstepping the boundaries of protection.

## 3.3 Access and Use of personal data in research projects

### 3.3.1 Attitudes towards the use of private data

Without exception, the participants thought of using private data in medicine as being of benefit when it could help prevent new diseases or epidemics, when developing new medicines or when addressing and solving global problems. One of the participants was even as ambitious as to argue that by utilising a big enough pool of personal data, one can even develop a panacea.

Conversely, a strongly negative attitude was expressed only in relation to the assumption that possessors of one's personal data may misuse it or abuse it, i.e. turning it into their own gain or profit.

### 3.3.2 Perspectives on consent

All of the participants shied away from discussing matters of consent as a prerequisite to using one's data. To them, consent appeared as a rather abstract notion that was taken for granted, i.e. one's data could not be used without a form of consent. Participants found difficult, however, to discuss the various forms of consent in a context. Instead, they referred to giving consent as the explicit, personal provision of consent for each particular request for the use of data. At the same time, they also viewed requests for consent as formal, since very often, at least in healthcare facilities, giving consent is not necessarily a choice, but rather a prerequisite. In this sense, participants seemed to be confused about giving consent for getting their personal data used/accessed, and giving consent as a form of understanding of the risks involved with a specific medical procedure.

Furthermore, most of the participants appeared rather distrustful of the formal procedures for giving consent. They were doubtful whether their data would actually (and only) be used for the purposes for which their consent was granted, and referred to the need of a specialised monitoring and controlling body, which would be ultimately responsible for safeguarding all collected data and for supervising how it is being accessed, by whom, and for what purpose.

Another perspective, voiced only by a single participant, was slightly broader in that consent was viewed as unnecessary if the requirement for the use of data comes from a public institution, and is linked to an emergency situation, whereby urgent action is needed in order to benefit the public at large - prevent a disease, respond after a natural disaster, etc. However, if the request is made by a private organisation, consent was seen as the only tool to prevent said organisation from obtaining one's data. In that case, most of the participants agreed that anything a private organisation would do with the data, would be linked to profit (and its own private gain), and therefore cannot be good.

### 3.3.3 Who may have access to personal data

Three different questions were elaborated that touched upon the issue of regulating access to personal data. There were two broad themes distinguishable in the discussions. One was that access to any data needs to be regulated in detail so that every time one's data is being accessed, one should be notified about both who accessed it, and for what purpose. Participants made it very clear that a clear mechanism should be in place that will enable one to get notified when any of his or her data is being accessed and used for anything.

Participants were more specific when they talked about particular types of access by particular institutions. For example, general practitioners (GPs) who need access to one's health records in order to exercise properly their profession were assigned a more special role. Due to the nature of their work, they were also considered as the ones who should be notified about and who should decide upon any third party requests to get access to one's data. When an employer needs access to a candidate's health record, it was suggested that candidate's GP should be the one to process that request and to decide whether any data would be shared. It was also the GP who is ultimately responsible to take care of anonymisation of data in the cases when data are requested for the purposes of scientific research. For the participants, it seemed appropriate that the GP serves as a "consent proxy".

Employers were one of the most frequently referred to types of data users during the interviews. There were a number of opinions that differed in the extent that access to data was given. A frequently shared position was that only the individuals themselves should decide how much data should be provided to employers, if any, without the employers having the right to demand any data. A slightly different position was that employers should have the right to access data about future or current employees, however they could only get it from the person involved, and not from a third party (which is, essentially, the currently existing

regulation with respect to newly appointed personnel). Some of the participants further insisted that employers should not be allowed to re-share data of their employees, not even anonymised data. An interesting addition to that was the suggestion that different types of employers should have different levels of access to data, i.e. for kindergartens a larger pool of data should be available and processed compared to a local administration office, for example. This further emphasised the belief shared by most of the participants that access to data is allowed by default if there is a chance that a prospective negative consequence be avoided.

At another table the participants insisted that only publicly funded organisations (i.e. government institutions and those funded by the state) may have access to personal data. In their view, public organisations are less likely to abuse the personal data that they have access to, while private organisations were seen as much more likely, mostly for the sake of profit. Nonetheless, some of the participants admitted, though hesitantly, that private organisations may also be given access to personal data should that be for the purposes of the public interest. Moreover, it was with private organisations only that participants thought about a requirement for consent - one that was completely ignored with regards to public organisations.

Some of participants further discussed specific cases of handling highly sensitive personal information, such as data about positive HIV status, cancer diagnoses and history, or certain psychiatric conditions. They considered this sensitive from the perspective of employment opportunity since revealing such information might lead to discrimination - in the office, in particular, but also within the community at large, in general. Therefore, the dominant opinion around the table was that such information should in general be kept confidential, and should only be revealed - on the initiative of a physician, before an employer has even requested it - if there would be a threat to third parties.

The majority of participants also agreed that research and scientific organisations should only be granted access to anonymised data, thus emphasising the conviction that anonymisation should be performed by an independent entity that is not related to the organisation using the data.

# 4 RECOMMENDATIONS

Following discussions during and after the interviewing process, a total of **16** raw problem statements were elaborated across the three tables during the consultation. At one of the tables, the participants could not easily make the distinction between a problem statement and a recommendation, so they provided a mixture of both over six separate statements. Following is a list of all original statements (as formulated by the citizens) in alphabetical order:

- A specialized public body – whether to have? Which one and with what powers?
- An information campaign on how to protect our own personal data
- Clear regulation about who can collect what data
- Clear rules for protection in case of misuse/abuse of personal data – who does what
- Control over the storage and destruction of information
- Discriminatory practices in using health record data by employers and insurers
- Information about who and for what purposes has access to our personal data
- Low efficiency of the existing legislation
- People are not adequately informed about what happens with their personal data.
- Personal meta-data
- Poor awareness among people of the possible risks in sharing personal data
- Protection of collective meta data
- Scope of responsibilities and efficiency of ethical committees
- The request for data should be motivated and the risks of using these data should be clear in advance
- Trading personal data
- Transparency on who uses our personal data, how, and for what purpose

Having analysed the problem statements across all tables, the 16 problems were reduced to a list of 10, based on similarity of focus, thus also highlighting some similarities across the tables. The following table presents (in alphabetical order) the resultant list of 10 key problem statements and how they were advanced at each table (an ***x*** in the cell indicates the problem was elaborated on the respective table; numbers are provided for easier referencing and do not indicate importance):

| | **Problem statement** | **Table 1** | **Table 2** | **Table 3** |
|---|---|---|---|---|
| **1** | Clear rules are needed for protection in case of misuse or abuse of personal data | x | | |
| **2** | Discriminatory practices in using health record data by employers and insurers still persist | | | x |
| **3** | Low efficiency of the existing data protection legislation | | | x |

| | Problem statement | Table 1 | Table 2 | Table 3 |
|---|---|---|---|---|
| **4** | Poor awareness among people of the possible risks associated with the use of personal data | x | x | x |
| **5** | Rules for the protection of collective meta-data are needed | | x | x |
| **6** | The control over the storage and destruction of information seems to be insufficiently regulated | | x | |
| **7** | The scope of responsibilities and the efficiency of ethical committees are not well defined | x | | |
| **8** | Trading personal data | | | x |
| **9** | Uncertainty about the need for a specialised public body and the range of its powers and responsibilities | | x | |
| **10** | Unclear/insufficient regulation about who can collect what data | x | | |

Only one of the problem statements was shared across the three tables (under #4), and one was elaborated at two of the three tables (#5). All others were unique to only one of the tables. However, while problem statements coming from tables 1 (where originally 6 statements were produced) and 2 (where 5 were produced) were each reduced down to 4, at table 3 a total of five problem different problem statements remained, reflecting a possibly richer discussions. Elaborated recommendations are listed below for each problem identified:

**#1. Clear rules are needed for protection in case of misuse or abuse of personal data**

***Recommendation***: Establish clear rules defining how protection is offered in cases when personal data are misused or abused, and specify the responsible body and the procedures to be put in place.

**#2. Discriminatory practices in using health record data by employers and insurers still persist**

***Recommendation***: Define, through regulatory measures, different ranges for the scope of data that employers and insurers would have access to, based on a specialised classification by profession;

Health records for specific diseases that may pose a threat to third parties should be ***proactively*** reported to employers and insurers by an authorised medical representative, rather than being requested.

**#3. Low efficiency of the existing data protection legislation**

***Recommendation***: Participants could not offer an actual recommendation to this, as they considered it a "likely" problem and were not aware of the existing legislation and specific regulations. However, they felt there was a need to improve on the legislative framework with regards to data protection.

**#4. Poor awareness among people of the possible risks associated with the use of personal data**

***Recommendation***: Ensure transparency on who requests access to one's personal data, how often, and for what purpose;

Organise awareness-raising campaigns, especially among students (at school) and focus on methods for prevention of data misuse; address motivation of people to know and protect their information rights (personal data);

Develop an online platform to enable the control of access to citizens' personal data;

Require personal consent everywhere when access to personal data is required;

Work with children and youth as a priority to educate them about the protection of personal data and their information rights.

**#5. Rules for the protection of collective meta-data are needed**

***Recommendation***: Develop coherent national policy targeting the protection of personal meta-data (data about a specific community of people); clearly define the range of data that is to be considered of high risk (such as ethnicity, nationality, etc.);

Ensure annual upgrades of the data protection technologies (including both software and hardware, when necessary);

Make it possible that the state should have the right to deny the provision of information;

Contribute to the creation of common EU legislation and rules for the export (sharing with third parties) of data and the handling thereof by the respective recipients.

**#6. The control over the storage and destruction of information seems to be insufficiently regulated**

***Recommendation***: Ensure that individuals have the ultimate authority on deciding how to keep and retain personal information; in the case of death, the heirs should be the ones to decide how to use the personal information; after a certain period of time personal data should be automatically deleted.

**#7. The scope of responsibilities and the efficiency of ethical committees are not well defined**

***Recommendation***: This was another "likely" problem that participants did not feel too knowledgeable about to give a specific recommendation. They were unaware of how, if at all, Ethical committees are assembled, are operating, and are making decisions, and did not easily understand the difference between an Ethics committee and a specialised government body for data protection.

**#8. Trading personal data**

***Recommendation***: Enforce strict EU and national regulation;

Improve awareness among people so they would know how to demand protection and from which relevant authorities;

Create an Information Platform that would be able to filter who can use what types of data and how;

Impose severe sanctions in case of misuse of personal data.

**#9. Uncertainty about the need for a specialised public body and the range of its powers and responsibilities**

***Recommendation***: Establish a specialised government body with competences in health care. It should be a multi-disciplinary, publicly funded organisation which is assembled in order to address specific cases.

**#10. Unclear/insufficient regulation about who can collect what data**

***Recommendation***: The request for data should be motivated and the risks of using these data should be clear in advance.

# 5 CONCLUSIONS

Provide your main conclusion from the meeting in half a page.

The participants enjoyed the meeting and were very positive about the experience. However, it was rather clear that the topic presents a complex challenge, mostly due to the fact that most, if not all, of the participants had not encountered any issues of privacy and data protection before, especially when it comes to research. Nobody knew about any of the provisions of the Law on Protection of Personal Data, nor was familiar with the mandates of the existing Commission for Personal Data Protection that has been in existence since 2002. In this line of reasoning, it is not surprising that one of the most pressing issues discussed by the participants was the need for an awareness raising campaign.

For most, if not all, of the participants, the event also provided a learning opportunity as they had never before considered the issues of privacy and data protection in such a detail. The informational material, as well as the questionnaire, highlighted a number of issues that participants had not thought about before, so they demonstrated high levels of engagement during the day, and the discussions were really lively.

It was evident that the topic of the event is generally poorly understood, and most of the discussion was easily steered away from the use of data in science and research. Instead, the participants would focus on more general issues of data protection, and spend considerable amount of time debating the need of special regulations, the high risks of data misuse by data administrators, and further expressed a wish there were a central state body to oversee everything related to (personal) data sharing and protection.

What questions issue was the cause of most discussion and what issue concerns was there the broadest agreement on?

Overall, participants demonstrated a great level of distrust towards some of the typical administrators of personal data, such as employers and insurers. Moreover, any administrator of personal data was seen as a potential offender who is somehow directing the use of personal data towards his or her own personal (financial) gains. Therefore, many of the participants seemed to expect that a special (government) body would be tasked with observing if data is properly stored and protected, and that body would also have punitive authority over any data misuse or abuse.

In general, all participants spend a lot of time discussing legislative or regulatory issues. However, this was in part due to the poor knowledge they had about the current legislation in

place, so they would easily imagine that a good piece of legislation and a set of relevant regulations would successfully address all issues. However, this can hardly be used as a measure of the efficiency of the current regulations. Instead, all participants agreed there was very little awareness – among both ordinary citizens and among the data administrators themselves – about how to properly ensure the protection of personal data.

The majority also agreed that if data is to be used in research, its purpose would have to be some kind of societal benefit or a noble cause. Nonetheless, everyone agreed that researchers and scientist should only be granted anonymised data, and should not have responsibility over the anonymisation themselves.

Another point of agreement was about having knowledge over who accesses one's data and for what purpose. Thus, for example, when an employer or a doctor accesses one's data – health records or employment files – the person affected should be alerted and should become aware that his or her data were accessed. No one from the participants was aware if there was any such functionality available at the moment, so it came out as a strong desire, along with a recommendation for its proper codification into the law.

Annexes

Please provide us with the filled in questionnaires.