

A Work Project, presented as part of the requirements for the Award of a Master Degree in Management from the NOVA – School of Business and Economics.

A Race for Maintaining Personal Data

- How to Manage consumers' data under the Right to Be Forgotten and the Right to Data Portability of the new EU GDPR -

ALEXANDRE SOARES DE OLIVEIRA LUCENA E VALE

N.º 27277

A Project carried out on the Master in Management Program, under the supervision of:

Professor Ana Paula Amaro

January 3rd 2018

Abstract

The phenomenon of Big Data is revolutionizing business and imposes the study of two underlying issues: data protection and economic value of personal data.

With the new EU Data Protection Regulation, the use of personal data by corporations has become more limited, giving individuals the right to ask from companies to delete their personal data or transfer it to other competitors.

Under these conditions, this preliminary study explores how individuals in the European Union view their new data protection rights and whether they put a price on their privacy, showing that a significant number is willing to make trade-offs.

Keywords: Big Data, Data Protection, Personal Data, Right to Be Forgotten

Table of Contents

1. Introduction.....	4
2. Literature Review	5
2.1. Big Data is a Big Deal	5
2.2. Personal Data Protection Regulation (in Europe)	7
2.2.1. A Brief Overview	7
2.2.2. The EU GDPR.....	8
2.2.3. Right to Data Portability and Right to Be Forgotten	9
2.3. Uncovering the value of Personal Data and Privacy.....	11
3. Research Questions and Methodology.....	14
4. Results and Discussion.....	17
4.1. Awareness of Right to Be Forgotten and Right to Data Portability	18
4.2. Likelihood of Exercising the Right to Be Forgotten and Right to Data Portability.....	20
4.3. Value of Right to Be Forgotten and Implicit Value of Personal Data.....	21
4.4. Terms of Use Declaration – Confirming Previous Findings	23
5. Final Conclusions and Study Limitations.....	24
6. References.....	25

1. Introduction

“We are living in the digital age.” This is an expression that probably everyone is accustomed by now. There are many technological trends that define our current digital times - one of them certainly being Big Data.

Big Data is a powerful concept that is revolutionizing the way businesses operate. Nevertheless, it raises some issues causing law makers to ensure the protection of personal data and economists to study the value of personal information.

With the new EU General Data Protection Regulation (GDPR) coming into force in May 2018, the existing limitations for companies to use data have become much stricter. The true impact of these measures is to some extent still unknown but - following the basic economic theories of supply and demand when there is a supply-induced scarcity of a good - it would be reasonable to expect that the price of personal data will increase. Namely, there are two new rights created – Right to Be Forgotten and Right to Data Portability – that can greatly affect data management strategies.

With this in mind, the economic experiment of this study aims at figuring out how consumers value their personal data within the context of these new formalized rights. The conclusions may be useful for companies who want to maintain personal data of their consumers for a longer period. The study will have the following structure: a brief literature review over the phenomenon of Big Data and on the underlying issues of Data Protection Law and the Value of Personal Data; a description of the methodology used for the economic experiment in this study regarding the new rights of the EU GDPR and their economic value, followed by results and discussion; and the final conclusions of the study as well as its limitations.

2. Literature Review

2.1. Big Data is a Big Deal

Big Data is a large volume of data or information that businesses deal with every day. The term gained its true meaning in the 2000s when it was formally linked to the three Vs: Volume, Velocity and Variety (*SAS, 2017*), when technology allowed for organizations to rapidly collect massive amounts of data, coming from all sorts of formats and sources, and store it in the so-called cloud systems.

But the relevance of big data does not only derive from the increase of information storage capacity. It is mainly due to advanced analytics systems and algorithms that were developed allowing to analyze and treat information in ways that were not possible with previous computational methods (*Shaw, 2014*).

The so-called “Big Data Revolution” started at the turn of the 21st century along with the internet rise and it exploded as more and more people started using connectable devices. Today it has become a daily life phenomenon.

In Europe, the Data Market shows some impressive numbers. The value of the overall data market – where digital data is exchanged as products or services – represented in 2016 more than 59 billion euro and it signified around two per cent of the European GDP with a clear upward tendency (*IDC and European Commission, 2017*).

Big data is affecting practically every industry in the economy (*IDC and European Commission, 2017*).

In the public realm, it can range from government issues - better managing utilities, traffic congestion and preventing crime - to education – improving students’ performance – and health – further studying the human genome to discover causes of diseases. The banking sector can use it

to monitor banking transactions, detecting fraud and enhancing compliance, the manufacturing sector can streamline its production process and the retail sector can improve its relations with its customers, personalizing their offers and make sure they stay loyal (*SAS 2017*).

All in all, big data paired with high end powered analytics can make someone do better decisions, having less costs and using less time while optimizing service. It is no wonder that almost every business has decided to make use of it.

There is data being recorded about almost every aspect of people's lives – from personal identification, location, genetic information and online purchasing habits. This has led some to believe that “personal data is the new oil of the internet and the new currency of the digital world” (*Kumeva, 2009*). It has become a new asset class. Companies such as Google and Facebook have entire businesses that run based on the use of personal data (*World Economic Forum, 2011*).

There are three types of data that have been defined by the recent Big Data literature (*World Economic Forum, 2011*):

- Volunteered data—created and shared by individuals, such as social network profiles
- Observed data – captured by recording the actions of individuals, such as the location data when using cell phones.
- Inferred data – data about individuals generated from the analysis of the previous two types of data, e.g., credit scores.

Some might view these phenomena of constantly sharing personal information as a way of improving our economies and upgrading our experiences online. As one does not pay in general to access the internet, sharing data could be viewed as a fair cost of this service (*Ehrenberg, 2014*). However, most of the scientific community does not see this as a clear issue. Sharing your personal data is not free of risks and of adverse consequences. It directly interferes with individuals' privacy

rights protected under law in most countries. These factors emphasize the need for the use of personal information to be, on the one hand, subject to regulation and, on the other hand, have a price linked to its disclosure, even with consent (*Ehrenberg, 2014*).

2.2. Personal Data Protection Regulation (in Europe)

2.2.1. A Brief Overview

Data Protection refers to the “legal control over access to and use of data stored in computers.” (*Oxford Dictionary, 2017*).

It dates back to the 1970s when computers suffered a great development leap which made them more and more capable of storing considerable amounts of data (*Rudgard, 2012*).

Although the recently created data processing methods allowed to correct economic deficiencies, it rapidly led to fears that would have an adverse effect on privacy of individuals. Privacy was already protected as a human right by many international legal instruments, namely in Universal Declaration of Human Rights (*Article 12 and 19*) and the European Convention of Human Rights (*Article 8 and 10*).

In Europe, the specific issue of protection of personal data stored in computers was subject to law scrutiny at a national level at first and then at an European Level - with two Resolutions and the Convention 108 from the Council of Europe (*Rudgard, 2012 and Resolutions of Council of Europe*) and several guidelines from the Organization for Economic Co-operation and Development (*OECD, 1980*).

At the European Union (EU) level, regulation only came later. The first rules on the protection of individuals regarding the processing of their personal data were set out in the Directive 95/46/EC. This issue was also later enshrined in the treaties of Lisbon (*Article 16 of the Treaty of the Functioning of the European Union*) and the Charter of Fundamental Rights of the EU (*Article 8*).

2.2.2. The EU GDPR

In order to answer the new technological developments of the data-driven world and to ensure the free movement of personal data within the internal market, the EU adopted in 2015 a regulation with the aim of creating consistency among data protection standards throughout the Union. The so called General Data Protection Regulation (GDPR) enters into force on May 25th 2018, bringing some significant changes to the data protection system. (Regulations are binding in every element and in every EU member-state, contrary to Directives that are only binding over results, leaving member-states to decide how to transpose rules into national law – article 288 TFEU).

It will have an increased territorial scope. The EU GDPR will not only apply to controllers and processors (those who are responsible for ordering and processing personal data) that reside in the EU but to all companies who process personal data of individuals residing in the Union, regardless of their location and of whether the processing takes place in the Union or not (*Article 3 of the EU GDPR*). This means, for example, that a company from the United States of America that deals with customers from the EU and processes their personal data will also be under this regulation.

There are also new rules for consent determining that the latter is only valid if the Terms of Use Declaration is clear and easy to read. The subject can withdraw his or her consent at any time, following article 7 of the EU GDPR. This comes after several published studies showing that most of the people do not read the Terms of Use Declaration before they give consent to share their data and complaints that the latter are too long and hard to read (*Obar, 2016 and Tsai, 2010*). In the economic experiment of this paper, the same evidence is presented (as it can be seen further ahead).

The EU GDPR creates more obligations to companies: they must implement appropriate technical measures to guarantee anonymity of data subjects; they have to keep registries proving compliance of all the obligations derived from the Regulation and, in some cases, prepare Privacy Impact

Assessments and appoint Data Protection Officers; they should provide information about the personal data being held to individuals. Any data breach that may cause harm to for the rights of individuals must be notified within 72 hours after the company becomes aware of it (*Article 33 of the EU GDPR*).

Companies in breach of EU GDPR obligations may now be fined up to 4% of the annual global turnover or 20 million euros, whichever is higher (*EU GDPR Portal, 2017*). These fines serve as a real deterrent for any business that might consider not complying with the rule.

2.2.3. Right to Data Portability and Right to Be Forgotten

Individuals see new rights being enshrined in the EU GDPR to protect their personal data. Two of the most important ones are the Right to Data Portability and the Right to Be Forgotten. These rights will represent in great part the subject of the economic experiment within this study, hence the need to analyze them in greater detail.

An introductory note that applies to both rights mentioned above is that companies - data controllers - must inform individuals - data subjects - about the existence of these rights and the possibility exercising them, requesting to erase the data or to transfer it to another data controller (*Article 13(2)(b) and article 14(2)(c) of the EU GDPR*).

Regarding the Right to Data Portability, article 20 of the EU GDPR creates an entire new right which allows “to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance” (*Article 20(1) of the EU GDPR*).

The underlying objective of right to data portability is to empower individuals regarding the way they can control and manage their own data, creating new means to transmit personal data from

one digital environment to another and possibly leading to more innovation and more competition (*Article 29 Data Protection Working Party, 2016*).

It includes two elements: a right to receive personal data from a data controller and to store it as the individual sees fit; a right to transmit personal data from one data controller to another (*Article 29 Data Protection Working Party, 2016*).

As to what kind of data should be included in this right to data portability, article 20(1) EU GDPR states that it must be data that the subject has given consent or that is based on the contract signed by him/her. It has to be data concerning the subject or that he/she provided to the data controller. Inferred data, as early defined, is not included in the scope of this article (*Article 29 Data Protection Working Party, 2016*).

For example, if a client of a bank decides to exercise the right to data portability, requesting to have access to personal information, data like mailing address, age, search history and location should be given. However, information about his credit score would not be covered as that is inferred from the analysis of the behavior of the data subject (the client) by the data controller (the bank)

The right to data portability cannot negatively affect the rights and freedoms of others and has to respect intellectual property rights and trade secrets (*Article 29 Data Protection Working Party, 2016*). It only applies to data processed by “automated ways”, which means that it does not include files on paper format.

Moving on to the Right to Be Forgotten, also called “Right to Erasure”.

The EU GDPR includes it in article 17 which refers that an individual might ask the data controller to erase his or her personal data.

This right had already been subject to a ruling of the European Court of Justice of 2014, after a Spanish citizen lodged a complaint against Google for maintaining online newspaper pages on search results, referring to a forced sale of his property to pay off his debts, therefore affecting his reputation (*European Commission, 2016*). The court ruled in his favor and Google was forced to comply with the decision and has accepted several other requests to remove URLs since then (*Macaulay, 2017*).

The Right to Be Forgotten was already briefly mentioned in the 1995 Data Protection Directive but only with the EU GDPR becomes formally recognized.

In order to exercise the Right to Be Forgotten, certain circumstances must be present (*Article 17 (1) of the EU GDPR*), namely that the personal data is no longer necessary for the original purposes of processing; that the data subject withdraws his/her consent to the data processing; or that the processing of data is not lawfully.

If data controllers have made the personal data public they might be obliged take the necessary measures to inform anyone else that is processing the data that the subject has requested to erase it (*Article 17 (2) of the EU GDPR*).

The right to have data erase must not be seen as an absolute right. Namely, it is not meant to be used to make “prominent people less prominent or making criminals less criminal” (*European Commission, 2016*). It must be balanced with compliance of legal obligations, other public interests and protection of the freedom of expression and freedom of the media.

2.3. Uncovering the value of Personal Data and Privacy

Along with data protection requirements there is another relevant issue that is related to Big Data which can be translated into the following problem:

“Should people be paid for the personal information they provide to companies?”

It seems logical to assume that in a data driven society where companies are increasingly dependent on information to conduct their business, individuals would hold some kind of leverage in this Big Data market.

Following that reasoning, some studies and experiences have been made to try to uncover the value of online privacy and personal information for both companies and individuals, although it is, to a large extent, an untapped subject.

Regarding the value of data for companies, there are quite some disparate results.

The Financial Times provides an interactive calculator to explore the value of someone's data. It states that the average person's data retails for less than one dollar when sold in a bundle of 1000 people (*Steel, 2013*). The value is bigger if the person is looking to buy a property or a car, if it has health problems or if it has a habit of buying online.

There are companies that actually buy data from individuals to sell to third parties as their core business (*e.g. Companies such as Datacoup pays 8 dollars a month for personal data*).

But some people have succeeded in selling their own data without the interference of any middlemen. By trying to sell their data via online auction or through Kickstarter - an Online platform that allows entrepreneurs to gather money to fund projects - they have managed to get more than 200 euros (*Ehrenberg, 2014*).

It seems quite difficult to truly understand the market value of such information.

Anyhow, with the entering into force of the EU GDPR, it is likely that the price of personal data is going to increase as the limitations to hold on to that information are much more significant.

Analyzing now the value that consumers give to privacy and to personal data, there have been a few studies and economic experiments made to uncover it. However, the price of information is

very hard to calculate for consumers as it can be quite subjective. Often consumers cannot make a rational decision when disclosing their information as they have no information about the market. Steinfield (2012) conducted an experiment in a virtual world game to try catching the value of anonymity preservation in that online platform. The study found there was a strong correlation between the sum of money offered to users and their willingness to grant access to Facebook profiles.

Turow, Henessy and Draper (2015) found that there is a misrepresentation over how marketers judge American consumers thinking they are willing to trade off their information for the benefits they get when marketers use that information “in the right way”. They conclude that the tradeoff happens because American consumers are resigned and feel powerless, with no control over their personal information.

3. Research Questions and Methodology

As already mentioned, the economic experiment of this study aims at figuring out how consumers value their personal data within the context of the Rights to Data Portability and the Right to Be Forgotten (especially the latter) under the new EU GDPR.

The first two research questions of this study are about assessing to what extent people living in the EU are aware of the Right to Be Forgotten and the Right to Data Portability. The null hypothesis is that the majority of people know that they possess these rights and the alternative hypothesis will be that less than the majority of people know that they possess these rights.

The next research question serves to determine how likely consumers will exercise the Right to Be Forgotten and the Right to Data Portability as a response measure to an inefficient service (given that they already know of the existence of these rights).

Finally, the main research question will be to determine whether consumers are willing to give up exercising their Right to Be Forgotten in exchange for an economic value. It will be also assessed if there is any relevant demographic variables that help explain who is more likely to trade-off their information.

In order to answer the research questions of this study, an economic experiment was conducted based on a survey.

The platform used to make this survey was Google Forms - a platform provided with Google accounts that allows to customize forms and save results on simple spreadsheets.

The audience of this survey is meant to be broad as these rights can be exercised by any individual that resides in the EU. Therefore, the only restriction that was made to respondents was that they live in the EU (and that they understand English, since the survey was conducted in this language).

Although there were no strict age limits in the survey, it was ensured that that the valid responses

would only come from people with the minimal age of 15 years old, due to the relative complexity of the issue of this study.

The respondents were sampled by convenience: a snowball sequence of friends and friends from friends. The conclusions are limited as the sample is not random, but the simplicity and reduced cost were considered strong arguments to allow for a preliminary study.

The respondents were characterized by age, gender, nationality, education level and online habits. The survey was structured in different sections. Each section was presented in different webpages. In the first section, respondents were asked whether they agreed with the Terms of Use of Google Docs. In the second session, they were asked to give personal information regarding demographics. Moving to the third session, they were asked about their online habits and then about their knowledge concerning the existence of a Right to Be Forgotten and a Right to Data Portability (questions in plain non-legal English). Respondents answered “Yes”, “No” or “I don’t know”.

The following section had two questions, resorting to hypothetical scenario creation that included the possibility of exercising the Right to Be Forgotten and the Right to Data Portability. The proposed scenario was that the respondent had subscribed an online movie streaming service, giving access to his/her personal data. However, there had been some technical problems with the service provided. Having read this scenario situation, the first question asked was about accessing the likelihood of exercising the rights above mentioned as a response to mediocre service. Respondents answered “Yes” or “No”. The second question of this section was preceded by another scenario building that derived from the first one: Respondents were told that they had decided to unsubscribe the movie streaming service and asked the company to erase their personal data. The company had responded proposing the following trade-off: give to the customer the equivalent to one month of subscription - 20 euros - if he/she decided to drop the request to erase

their personal data. Respondents were then asked if they would accept that trade-off or not. In this manner, a way was found to reasonably isolate the value that customers can give to their Right to Be Forgotten and, implicitly, to their personal data.

However, if the survey would end here, it could only be assessed if consumers would value their data for equivalent of 20€. To cover the possibility of waiving the exercise of their right to erasure and their personal data for more than 20€, another section was added. The respondents that answered “No” to the 20€ offer, would be confronted with another question asking if they would drop their request to delete personal data in exchange for more money. If they answered “Yes”, it was asked to state an amount which they would accept to trade their personal data.

The survey ended with a question asking whether or not respondents had read the Terms of Use Declaration showed in the very beginning. This shall not be considered as a research question of this study. It will serve only to confirm what many studies have already concluded that the clear majority of people do not read these declarations.

To perform the analysis of the collected data, different statistical tests were used.

To measure the statistical value of all the answers and the correspondent percentages, confidence intervals were calculated for each question.

To assess whether most people were aware of the new data protection rights, a one-tail significance test for hypothesis testing was conducted. It was considered that a value of $p < 0.01$ was statistically significant. The “Yes” answers counted as being aware of the existence of those rights and the “No” and “I don’t know” counted as not being aware of those rights.

To test for independence between variables, a contingency analysis was made conducting a chi-squared test of independence as only categorical and discrete variables are being considered. In this case, it was considered that a value of $p < 0.05$ was statistically significant.

4. Results and Discussion

Although there were several categories presented per variable in the survey (excluding gender), it was decided to decrease each variable to two categories in order to have more statistically significant results. In terms of age, the two intervals selected were “under 45 years old” and “45 years old or more”. The reason for this distinction lays in the fact that it is considered people under 45 years old (born in 1973 (appointed by several as the year it was invented the first personal computer) or after), who represent Millennials and late Generation X, have lived in contact with computers, the internet and the rest of the digital world almost all their lives and are in general more tech savvy than older generations. Regarding nationality, the categories selected were “Portuguese” and “non-Portuguese” due to the high number of Portuguese respondents. Concerning education level, the two categories selected were “High School or Bachelor Degree” and “Master or Doctoral Degree”. Finally, regarding online habits, answers were divided between those who buy online once a month or more (considered to be regular online consumers) and those who buy online less than once a month or never.

A total of 140 people responded to the survey for this economic experiment. In terms of gender 55,7% were female and 44,3% were male. Participants were mostly under 45 years of age (76,4%) and Portuguese (73,4%). Regarding education, 36,4% have High School or Bachelor Degree and 63,6% have Master’s Degree or PHD. Finally, regarding frequency of online habits, 68,6% of respondents buy online at least once a month and 31,3% buy online less than once a month or never.

4.1. Awareness of Right to Be Forgotten and Right to Data Portability

Only 25% of the participants stated that they know they have the Right to Be Forgotten while the other 75% responded “No” or “I don’t know” (Table I). This can serve as a good indicator that in fact *most people do not know they can ask companies to erase their personal data.*

A one-tail significance test was made to assess whether in fact the majority of the people did know about this right. The null-hypothesis was easily rejected – $p < 0.001$ ($Z = -5.91$ and critical value = $-2,32$ - with 99% confidence level). Therefore, there is strong statistical evidence to support the claim that less than 50% of the people are aware of the Right to Be Forgotten.

1. Awareness of Right to be forgotten (%)			
Variables	I don't know	Yes	No
Male	70.97%	20.97%	8.06%
Female	57.69%	28.21%	14.10%
<45	64.42%	26.92%	8.65%
equal or > 45	56.25%	21.88%	21.88%
Portuguese	61.76%	26.47%	11.76%
Foreigner	67.57%	21.62%	10.81%
HS or BA	66.67%	19.61%	13.73%
MS or PHD	61.80%	28.09%	10.11%
Buy online 1/month or >	60.64%	27.66%	11.70%
Buy online < than 1/month	69.77%	18.60%	11.63%
SubTotal	63.57%	25.00%	11.43%

Table 1: Awareness of Right to Be Forgotten (%)

Table 2 shows even more evidently that respondents are not aware of their data protection rights. The vast majority responded “No” or “I don’t know” to whether they have a Right to Data Portability and only 10,71% responded they knew. Again, testing whether one could say the majority of people know they have the Right to Data Portability, the null hypothesis was also rejected – $p < 0.001$ ($Z = -9.3$ and critical value = $-2,32$ - with 99% confidence level).

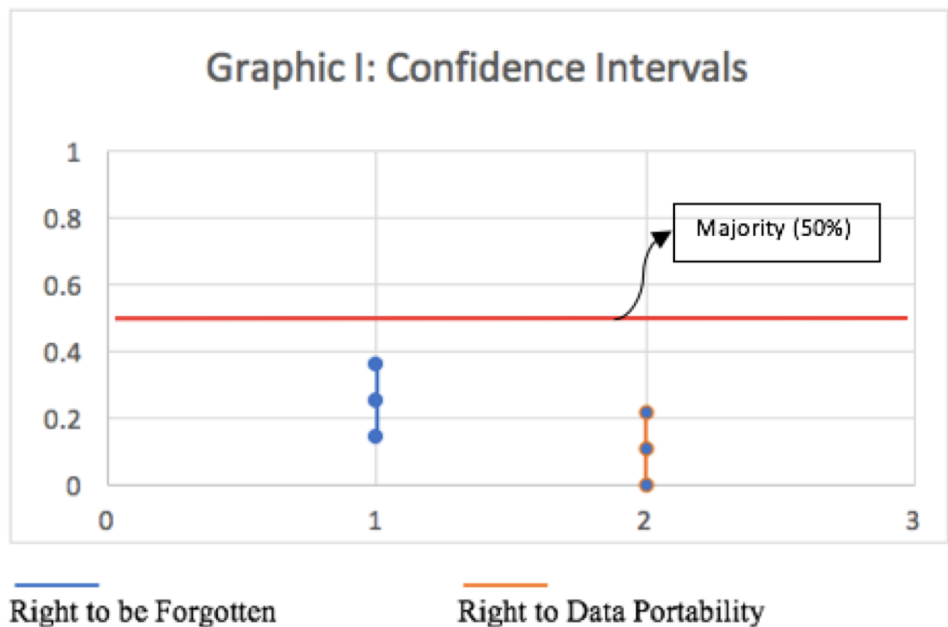
For both questions the difference among the variables was non-significant, after conducting contingency analysis for every variable..

2. Awareness of Right to Data Portability (%)			
Variables	I don't know	Yes	No
Male	75.81%	8.06%	16.13%
Female	67.95%	12.82%	19.23%
<45	73.08%	9.62%	17.31%
equal or > 45	65.63%	12.50%	21.88%
Portuguese	72.55%	10.78%	16.67%
Foreigner	67.57%	10.81%	21.62%
HS or BA	76.47%	7.84%	15.69%
MS or PHD	68.54%	12.36%	19.10%
Buy online 1/month or >	67.02%	12.77%	20.21%
Buy online < than 1/month	79.07%	6.98%	13.95%
SubTotal	71.43%	10.71%	17.86%

Table 2: Awareness of Right to Data Portability (%)

τ

In Graphic I, one can observe the 99% confidence intervals of our results regarding the two rights mentioned above. Again it is clear that most people are not aware of their existence, as the confidence intervals are located below the majority line.



Graphic 1: Confidence Intervals of Awareness of Right to be Forgotten and Right to Data Portability

4.2. Likelihood of Exercising the Right to Be Forgotten and Right to Data Portability

Regarding the probability of exercising the Right to Be Forgotten and Right to Data Portability, one can see in Table 3 that a big majority of people would consider exercising these rights as a response measure to mediocre service (in this case of online movie streaming service). More precisely, 76,4% of people answered they would ask the hypothetical company to erase their personal data or transfer it to another company, while 23,6% said they wouldn't.

3. Likelihood of Exercising Right to be forgotten						Contingency Analysis (χ^2)
Variables	Categories	Yes	No	SubTotal	Total	
Gender	Male	88.7% (55)	11.3% (7)	62	140	p= 0.002
	Female	66.7% (52)	33.3% (26)	78		
Age	<45	71.2% (74)	28.8% (30)	104	136	p= 0.008
	equal or > 45	93.8% (30)	6.3% (2)	32		
Nationality	Portuguese	77.5% (79)	22.5% (23)	102	139	p= 0.58
	Foreigner	73.0% (27)	27.0% (10)	37		
Education	HS or BA	80.4% (41)	19.6% (10)	51	140	p= 0.4
	MS or PHD	74.2% (66)	25.8% (23)	89		
Online Habits	Buy online 1/m or >	75.5% (71)	24.5% (23)	94	137	p= 0.65
	Buy online <1/m	79.1% (34)	20.9% (9)	43		
	SubTotal	76.4% (107)	23.6% (33)			

Table 3: Likelihood of Exercising Right to Be Forgotten and Right to Data Portability – Percentage (n° of respondents)

After seeing these results, one could argue that once more people start being aware of these rights, there is a great chance companies will see more requests to erase or disclose personal data to others, thus having a big impact on business and data management practices.

When conducting contingency analysis, recurring to the Chi-square test of independence, some interesting facts come to surface. Out of all the variables included in the study, two seem to have some relevance explaining the answers for this question. The first one being Gender. It seems that male are more disposed to exercise their new data protection rights than women (p=0.002).

The other relevant variable is Age. It seems that younger people (<45 years old) are less likely to exercise their Right to Be Forgotten and Right to Data Portability than older people (45 years old or more). It could be due to the fact that younger people are more comfortable sharing their personal data and do not care as much for that good as older generations.

4.3. Value of Right to Be Forgotten and Implicit Value of Personal Data

About 23,7% of the respondents answered they would accept to drop their requests for the online movie streaming company to erase their personal data in exchange for the equivalent of 20€ (one month of free subscription) (Table 4). 76,3% of the respondents did not accept the trade-off.

4. Trading your data for 20€						Contingency Analysis (χ^2)
Variables	Categories	Yes	No	SubTotal	Total	
Gender	Male	32,8% (20)	67.2% (41)	61	139	p= 0.027
	Female	16.7% (13)	83.3% (65)	78		
Age	<45	28.9% (30)	71.1% (74)	104	136	p= 0.024
	equal or > 45	9.4% (3)	90.6% (29)	32		
Nationality	Portuguese	23.8% (24)	76.2% (77)	101	138	p= 0.69
	Foreigner	21.6% (8)	78.4% (29)	37		
Education	HS or BA	20.0% (10)	80.0% (40)	50	139	p= 0.43
	MS or PHD	25.8% (23)	74.2% (66)	89		
Online Habits	Buy online 1/m	22.3% (21)	77.7% (73)	94	136	p= 0.60
	Buy online < th	26.2% (11)	73.8% (31)	42		
	SubTotal	23.7% (33)	76.3% (106)			

Table 4: Drop request to exercise Right to Be Forgotten in Exchange for the equivalent of 20€
Percentage (n° of respondents)

It can be stated with a 95% confidence level that between 15,4% and 32% of people would accept this offer. Although it is a fairly wide confidence interval, it serves to show that some people are in a way willing to trade their personal data for as much as 20€. This might be useful for companies to better understand the personal data market and help them redesign business strategies in times when there is a greater need for this kind of information.

Running contingency analysis again for all the variables, it was found that the same two as the previous question are relevant to explain the results at hand: Gender and Age. One can thus say that male are more likely than women to accept the trade-off to get the equivalent of 20€ in exchange for waiving the exercise of data protection rights (p=0.027). Meanwhile, younger generations are also more willing to trade their data than older ones (p=0.024). There does not seem to be a simple explanation for the gender difference. Regarding age, it would be reasonable to say, in the line of what was previously stated, that younger people, who are more at ease with technology, are less afraid of sharing their data than older people for a reasonable amount.

In Table 4 one could only see if respondents would accept to trade the exercise of their Right to Be Forgotten in exchange for the equivalent of 20€. However, the scenario where one would accept to trade this right for more than 20€ was left to cover. In table 5, one can see precisely the results for that premise.

6. Admitting an Economic Value to personal data (20€ or more)					Contingency Analysis (χ^2)
Categories	Yes	No	SubTotal	Total	
Male	59.0% (36)	41.0% (25)	61	139	p= 0.004
Female	34.6% (27)	65.4% (51)	78		
<45	49.0% (51)	51.0% (53)	104	136	p= 0.25
equal or > 45	37.5% (12)	62.5% (20)	32		
Portuguese	46.5% (47)	53.5% (54)	101	138	p= 0.53
Foreigner	40.5% (15)	59.5% (22)	37		
HS or BA	38.0% (19)	62.0% (31)	50	139	p= 0.19
MS or PHD	49.4% (44)	50.6% (45)	89		
Buy online 1/m or >	52.1% (49)	47.9% (45)	94	136	p= 0.02
Buy online < 1/m	31.0% (13)	69.1% (29)	42		
Subtotal	45.3% (63)	54.7% (76)			

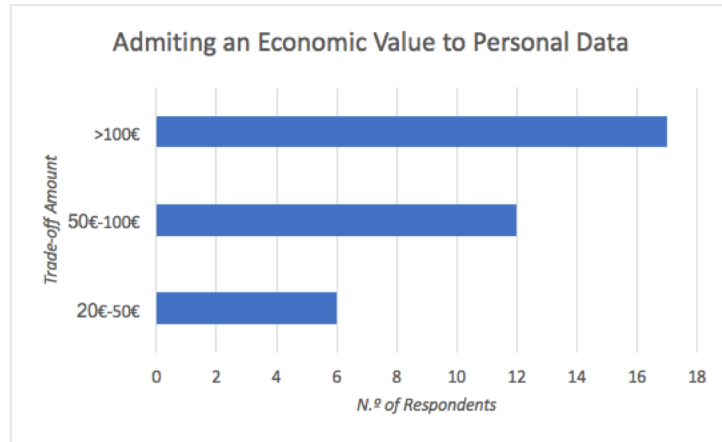
Table 5: Admitting an Economic Value to Right to Be Forgotten and Personal Data - Percentage (n° of respondents)

With no surprise, the amount of people who would accept the trade-off increases to 45,3%, with a confidence interval ranging from 37% to 53,6% (Table 5). It seems that almost half of the people would give an economic value to the exercise of the right to erase personal information.

When undergoing the Chi-square test of independence for all variables it was found again that men tend to trade their personal data more easily than women (p=0.004). The fact that difference in results regarding age is no longer relevant is noteworthy, possibly meaning that older generations also give an economic value to the exercise of their Right to Be Forgotten but that value tends to be higher than for younger generations. Finally, there is a new relevant variable emerging – frequency of online habits. It can be said that people who buy online once a month or more are more likely to trade-off their personal data than people who buy online less often (p=0.02).

Respondents who admitted giving an economic value to the exercise of the Right to Be Forgotten were asked to indicate a price for which they would accept the trade-off.

The values are very dispersed, ranging from 20€ to 10.000€. In graphic 2, one can observe that about half the people are willing to trade the exercise of their data protection rights for less than 100€. The other half is only willing to do it for more than 100€.



4.4. Terms of Use Declaration – Confirming Previous Findings

One last comment on the Terms of Use Declaration which was also a part of the survey presented to the participants. The results only confirm what previous studies have shown that the clear majority of people still do not read these declarations, resulting many times in giving consent without being fully aware of what personal data they are giving access to.

Figure 1 shows that 92,9% (130) of the people responded that they did not read the Terms of Use Declaration, while only 10 people (7,1%) of the 140 respondents say they did.

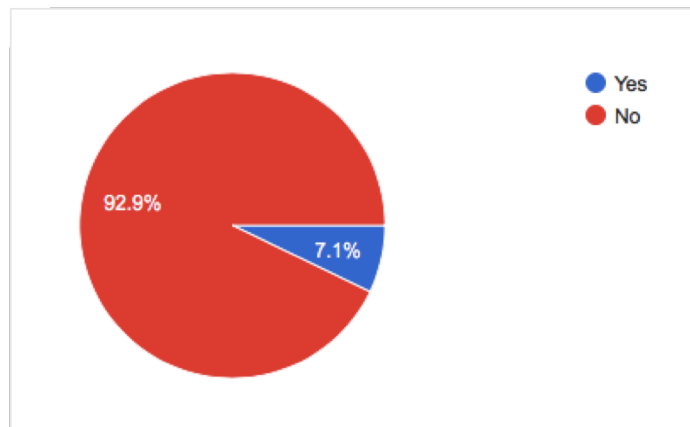


Figure 1: Response to whether the respondent has read the Terms of Use Declaration

5. Final Conclusions and Study Limitations

Based on this study sample, the new Rights to be Forgotten and Data Portability of the EU GDPR seem to be largely unknown to *people residing in the EU*. However, with the entering into force of this new regulation in just a few months' time this situation may well change.

Companies should be ready for this scenario, specially because once being aware of these rights, individuals are very much willing to exercise them.

In a world where personal information is becoming more and more important for business while the means to maintaining it are becoming increasingly limited, this study served to show that there is a price for which companies can afford to convince at least part of their consumers to retain their personal data. Companies might view this as an opportunity to review their business models and big data management policies.

Nevertheless, this study comprises some severe limitations.

The survey made in this study runs some risk of selection bias. Because it was chosen to analyze the population residing in the EU, there might have been some members of the population that are underrepresented, particularly people with 45 years old or more, given that the number of responses is limited and not always evenly distributed.

Also, due to the relative complexity of the issue, there might have been some response bias, with some participants not fully understanding the questions and choosing to behave differently in real-life. An effort was made however to simplify the questionnaire as much as possible whilst keeping it precise and real.

This piece of research should be considered as a preliminary approach to the subject and further studies should continue to be made on this increasingly relevant topic. This will allow to profit from this digital world that we live in while making sure it does not cause serious harm.

6. References

Articles

- Ehrenberg, Billy. 2014. "How much is your personal data worth" *The Guardian*. Accessed September 2017. <https://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth>
- Macaulay, Thomas. 2017. "What is the Right to Be Forgotten and where did it come from?" *Techworld, IDG* Accessed October 2017. <https://www.techworld.com/data/could-right-be-forgotten-put-people-back-in-control-of-their-data-3663849/>.
- Obar, Jonathan and Oeldorf-Hirsch, Anne. 2016. "The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services" *York University. Working paper*.
- Rudgard, Sian. 2012. "Origins and Historical Context of Data Protection Law" in *European Privacy*. International Association of Privacy Professionals (IAPP).
- Shaw, Jonathan. 2014. "Why Big Data is a Big Deal" *Harvard Magazine*.
- Steel, Emily et al. 2013. "How much is your personal data worth?" *Financial Times*. Accessed October 2017. <http://ig.ft.com/how-much-is-your-personal-data-worth/>
- Steinfield, Nili. 2015. "Trading with Privacy: the Price of Personal Information" *Emerald Insight*.
- Tsai, Janice Y. et al. 2010. "The effect of online privacy information on purchasing behavior: an experimental study" *Carnegie Mellon University. (Pre-Publication version)*.
- Turow, Joseph et al. 2015. "The tradeoff Fallacy: How marketers are misrepresenting American Consumers and Opening them up to Exploitation" *University of Pennsylvania*.

Institutional Sources

- Article 29 Data Protection Working Party. 2016. "Guidelines on the Right to Data Portability".
- European Commission. 2016. "Factsheets on the "Right to Be Forgotten ruling (C-131/12)".
- European Commission and IDC. 2013. "European Data Market SMART 2013/0063." Accessed September 2017 <https://ec.europa.eu/digital-single-market/en/news/smart-20130063-study-european-data-market-and-related-services>.
- European Commission Pres Release Database. 2009. "Meglena Kumeva (European Commissioner for Consumer Protection) Speech of 31 March 2009."
- EU GDPR Portal. 2017. "GDPR Key Changes". Accessed October 2017. <https://www.eugdpr.org/key-changes.html>.
- Organization for Economic and Social Development. 1980. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data".
- Oxford Dictionary online.
- Statistical Analysis System. 2017 "Big Data: What it is and why it matters". Accessed October 2017 https://www.sas.com/en_us/insights/big-data/what-is-big-data.html.
- World Economic Forum. 2011. "Personal Data: The Emergence of a New Asset Class".

Legislation

- 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 (OJ L 281, 23.11.1995, p. 31).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Resolutions 73/22 and 74/29, establishing principles for the protection of personal data in auto- mated databanks in the private and public sectors.
- The Universal Declaration of Human Rights and The European Convention of Human Rights.
- Treaty of the European Union (TEU) and Treaty of the Functioning of the European Union (TFEU).

Annex

A. Right to be Forgotten and Data Portability (Questions)

Section 1

Terms of Use of Google Docs:
(...)

If you agree with the Terms of Use, please click "Agree" to start answering this survey:

- Agree
-

Section 2

Please answer the following

Please state your age range:

- 0-17
- 18-30
- 30-45
- 45-54
- 55+

Please state your gender:

- Male
- Female

Please state where you come from:

- Portugal
- Other European States
- Outside Europe

Please state your Education Level:

- High School
 - Bachelor Degree (Licenciatura)
 - Master's Degree
 - Doctor's Degree
-

Section 3

How often do you make online purchases?

- Very Often (almost Every day)
- Often (1 per week)
- Sometimes (1 a month)
- Rarely (1 a year)
- Never

In Europe, can you ask from the companies where you make purchases online to delete your personal data that they have stored?

- Yes
- No
- I don't know

In Europe, can you ask from the companies where you make purchases online to transfer your personal data to another company (e.g. a competitor)?

- Yes
 - No
 - I don't know
-

Section 4

Imagine the following scenario 1

You have subscribed a service for streaming movies and TV series online from the company "XWezite". When subscribing, you allowed the company access to your personal data.

You have been fairly satisfied with the service provided for the past few months but recently you have experienced some technical problems that prevented you from using the service from time to time.

Knowing that you have the right to ask the company to erase your data (a good that is valued on the market) or to transfer the data to a company's competitor, would you consider using this right as a response for the mediocre service provided by "XWezite"?

- Yes
- No

Imagine the following scenario 2

Seeing no big changes in the service provided by "XWezite", you have decided to unsubscribe the service and you asked for the company to erase your data.

In response, the company apologizes for the trouble caused and proposes a trade off: The company will give you the equivalent to one month of subscription (20 euros) if you decide to drop the request to erase your personal data. Would you accept the company's offer?

- Yes
- No

Section 5

If you answered "No" to the previous question, would you accept to drop your request to erase your data if the company would give you more money?

- Yes (depending on the amount)
- I would never accept to drop the request to erase my data

If you answered "Yes" to the previous question, can you indicate a rough amount (€) for which you would accept to drop your request for the company to erase your data?

(fill the blank)

Section 6

Did you read all the Terms of Use Declaration that was presented to you in the beginning of this survey?

- Yes
- No

Thank you for answering this survey! Please don't forget to click "send"

You have just contributed to the progress of research and science. It was that easy. Cheers!

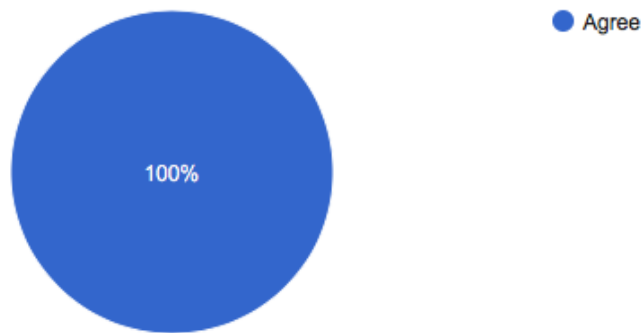
B. Right to be Forgotten and Data Portability (Answers)

Section 1

Terms of Use of Google Docs:
(...)

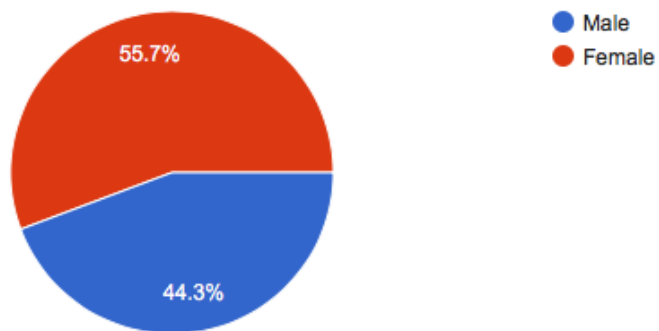
If you agree with the Terms of Use, please click "Agree" to start answering
this survey

137 responses



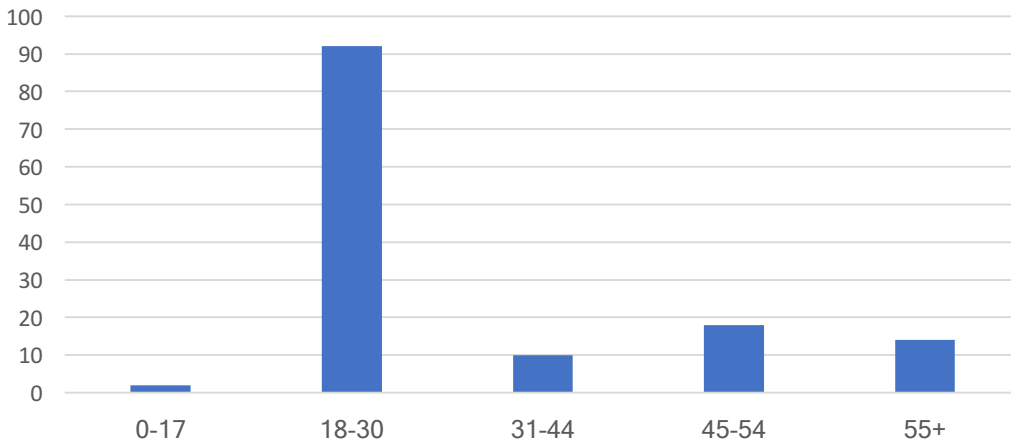
Please state your gender:

140 responses



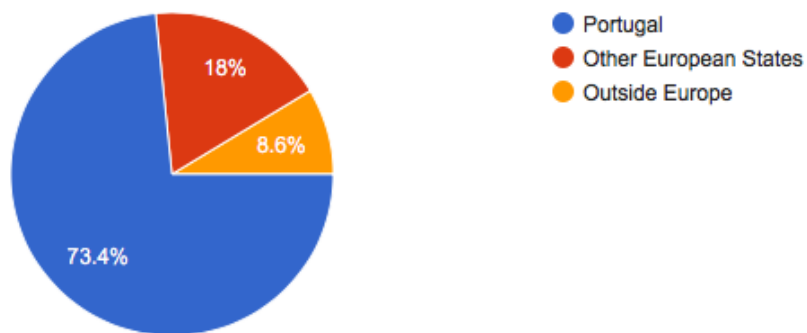
Please State Your Age Range:

136 responses



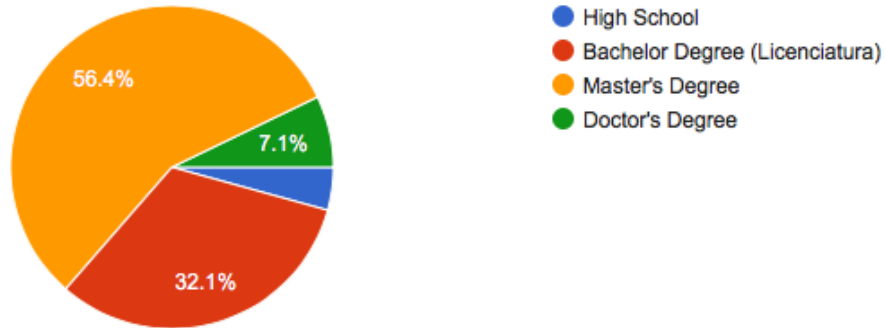
Please state where you come from:

139 responses



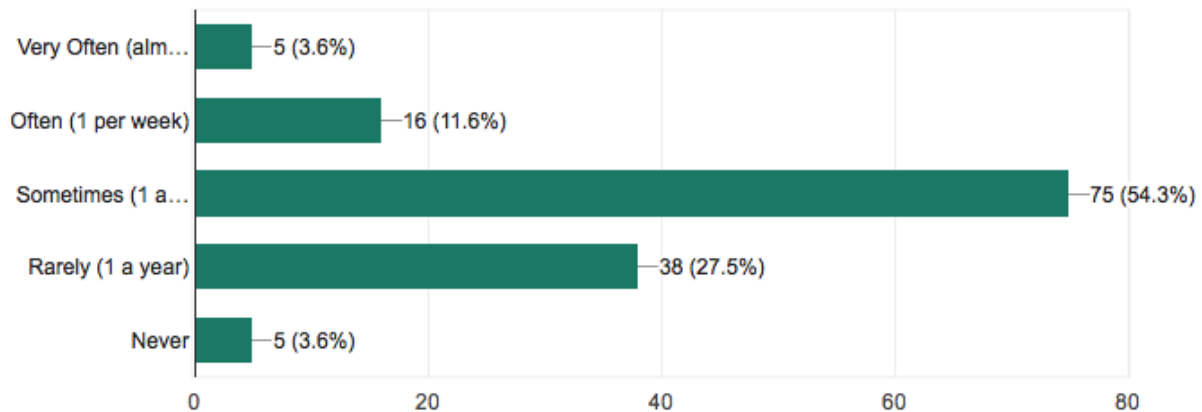
Please state your Education Level:

140 responses



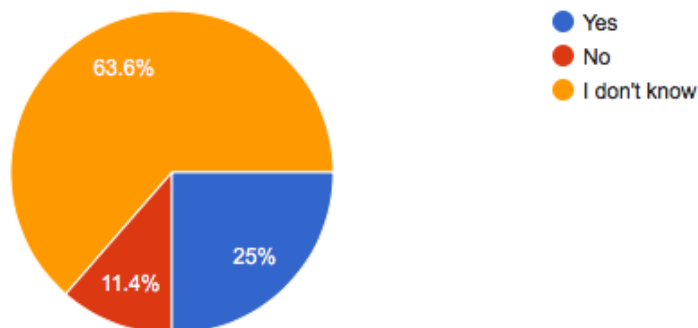
How often do you make online purchases?

138 responses



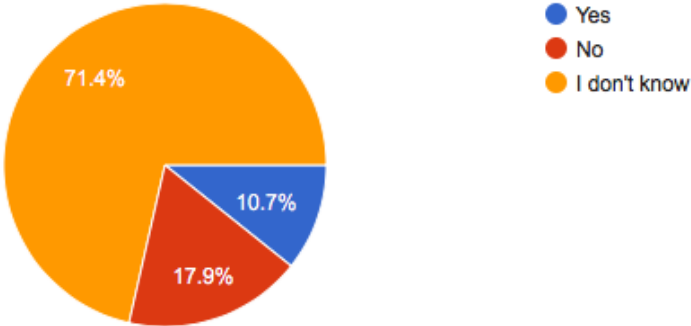
In Europe, can you ask from the companies where you make purchases online to delete your personal data that they have stored?

140 responses



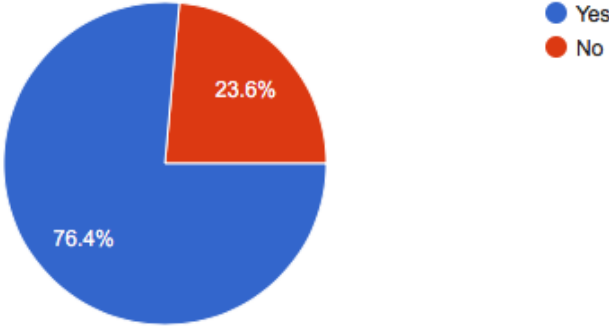
In Europe, can you ask from the companies where you make purchases online to transfer your personal data to another company (e.g. a competitor)?

140 responses



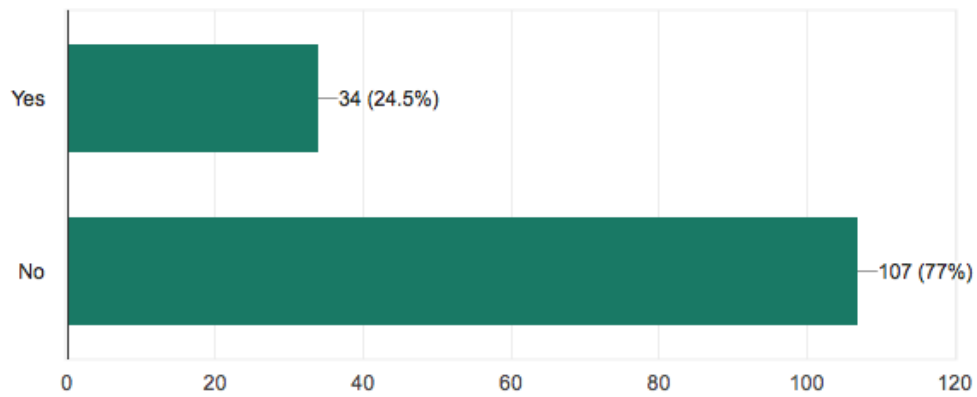
Imagine the following scenario 1

140 responses



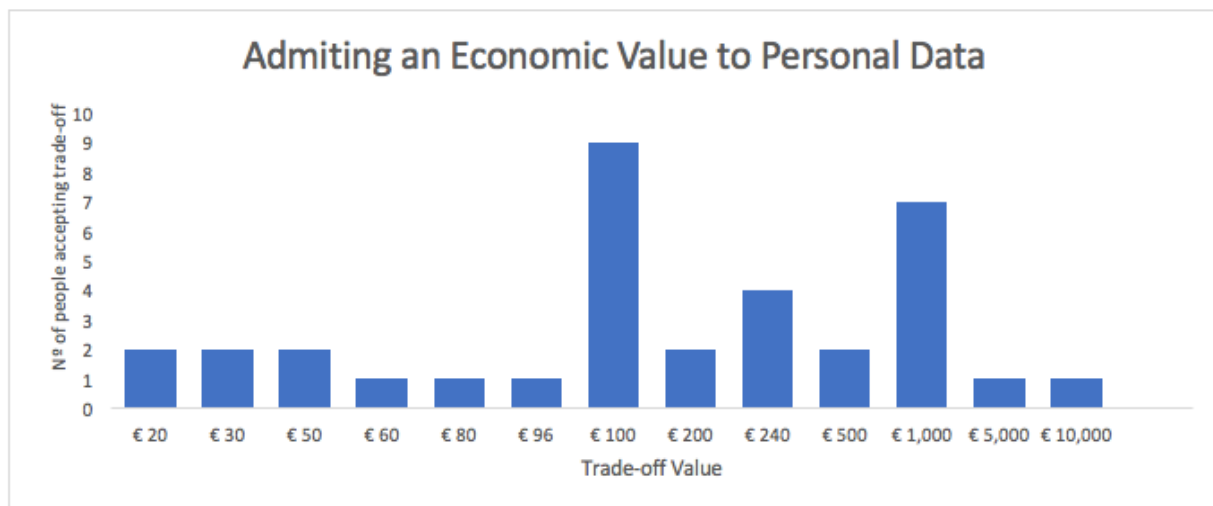
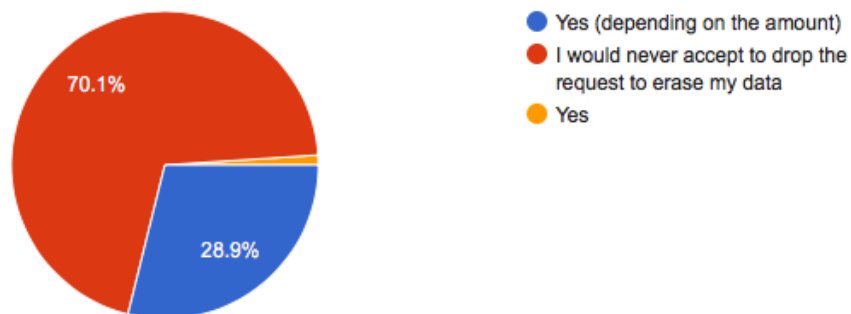
Imagine the following scenario 2

139 responses



If you answered "No" to the previous question, would you accept to drop your request to erase your data if the company would give you more money?

97 responses



C.Significance Tests (using STATA)

Awareness of Right to Be Forgotten

```
. ztesti 140 0.25 0.5 0.5, level(99)
```

One-sample z test

	Obs	Mean	Std. Err.	Std. Dev.	[99% Conf. Interval]	
x	140	.25	.0422577	.5	.1411513	.3588487

mean = mean(x)

z = -5.9161

Ho: mean = 0.5

Ha: mean < 0.5

Pr(Z < z) = 0.0000

Ha: mean != 0.5

Pr(|Z| > |z|) = 0.0000

Ha: mean > 0.5

Pr(Z > z) = 1.0000

Awareness of Right to Data Portability

```
. ztesti 140 0.1071 0.5 0.5, level(99)
```

One-sample z test

	Obs	Mean	Std. Err.	Std. Dev.	[99% Conf. Interval]	
x	140	.1071	.0422577	.5	-.0017487	.2159487

mean = mean(x)

z = -9.2977

Ho: mean = 0.5

Ha: mean < 0.5

Pr(Z < z) = 0.0000

Ha: mean != 0.5

Pr(|Z| > |z|) = 0.0000

Ha: mean > 0.5

Pr(Z > z) = 1.0000

Likelihood of Exercising Right to Data Portability and Right to Be Forgotten – Confidence Interval

```
. ztesti 140 0.7643 0.5 0.5
```

One-sample z test

	Obs	Mean	Std. Err.	Std. Dev.	[95% Conf. Interval]	
x	140	.7643	.0422577	.5	.6814764	.8471236

mean = mean(x)

z = 6.2545

Ho: mean = 0.5

Ha: mean < 0.5

Pr(Z < z) = 1.0000

Ha: mean != 0.5

Pr(|Z| > |z|) = 0.0000

Ha: mean > 0.5

Pr(Z > z) = 0.0000

Trading your Data for 20€ - Confidence Interval

```
. ztesti 139 0.2374 0.5 0.5
```

One-sample z test

	Obs	Mean	Std. Err.	Std. Dev.	[95% Conf. Interval]	
x	139	.2374	.0424094	.5	.154279	.320521

mean = mean(x) z = -6.1920

Ho: mean = 0.5

Ha: mean < 0.5	Ha: mean != 0.5	Ha: mean > 0.5
Pr(Z < z) = 0.0000	Pr(Z > z) = 0.0000	Pr(Z > z) = 1.0000

Trading your data for more than 20€ - Confidence Interval

```
. ztesti 139 0.4532 0.5 0.5
```

One-sample z test

	Obs	Mean	Std. Err.	Std. Dev.	[95% Conf. Interval]	
x	139	.4532	.0424094	.5	.370079	.536321

mean = mean(x) z = -1.1035

Ho: mean = 0.5

Ha: mean < 0.5	Ha: mean != 0.5	Ha: mean > 0.5
Pr(Z < z) = 0.1349	Pr(Z > z) = 0.2698	Pr(Z > z) = 0.8651