



# State of Privacy Report 2015



# Contents

	<b>Introduction</b>	<b>02</b>
<b>01</b>	<b>The Depth of Security Concern</b>	<b>05</b>
<b>02</b>	<b>The Data Trust Gap</b>	<b>19</b>
<b>03</b>	<b>Where Does The Responsibility Lie?</b>	<b>27</b>
<b>04</b>	<b>The Future of Data Privacy</b>	<b>35</b>
	<b>Biographies</b>	<b>44</b>

# State of Privacy Report 2015

**Data is fundamental to the functioning of our economy and society, and the protection of information has become the climate change issue for the born-mobile generation.**

In the next year, we are likely to see the European institutions adopt the new General Data Protection Regulation (GDPR) reform, and implement a framework designed to transform data governance in the EU. The new legislation will replace an existing structure that has been in place since 1995, a time that was in technology terms, prehistoric. Although necessary, such enormous change is naturally making many businesses slightly weary of the amount of disruption at stake.

The changes will ensure organisations have to adhere to new requirements around the processing of personal data, and introduce stricter rules around compliance. This is challenging even for the most informed, and has raised concerns over complexities around new information management processes, increasing costs and even question marks over career security. Although change is sometimes feared as painful,

it is widely recognised that these measures are necessary for people to realise the true potential of the internet and new technologies, while putting appropriate safeguards in place to ensure personal privacy is protected.

Symantec's State of Privacy report offers a snapshot of current perceptions on data privacy, and reveals that people don't believe businesses and governments are doing enough to keep their information safe. It also provides guidance on how businesses can address consumer concerns. We surveyed over 7,000 respondents across seven European markets; UK, France, Germany, Denmark, Spain, Netherlands and Italy and learned nearly 60 per cent have experienced a data protection issue in the past. Our findings suggest that businesses and governments have an opportunity to strengthen trust with Europeans by implementing aggressive security measures and assuring people that their data is gathered, stored and used responsibly.

Additionally, the report explores the role people play in securing their own information and their attitudes

about what their data is worth. Not surprisingly, our findings reveal that there is confusion about where to turn for help and who should be accountable for keeping information protected.

We've divided the report into four sections to look at the various approaches organisations and the public sector can take to help Europeans feel more at ease with how their data is being used, where it is stored, and what impact it has for wider society.

We have also spoken to experts within the industry to provide insight and suggestions on how businesses can improve their data privacy position.

**Darren Thomson**  
CTO and VP of technology  
EMEA Symantec



# The Depth of Security Concern

01

**The State of Privacy research identifies concern about the security of Europeans' data, and this mistrust extends across all industry sectors.**

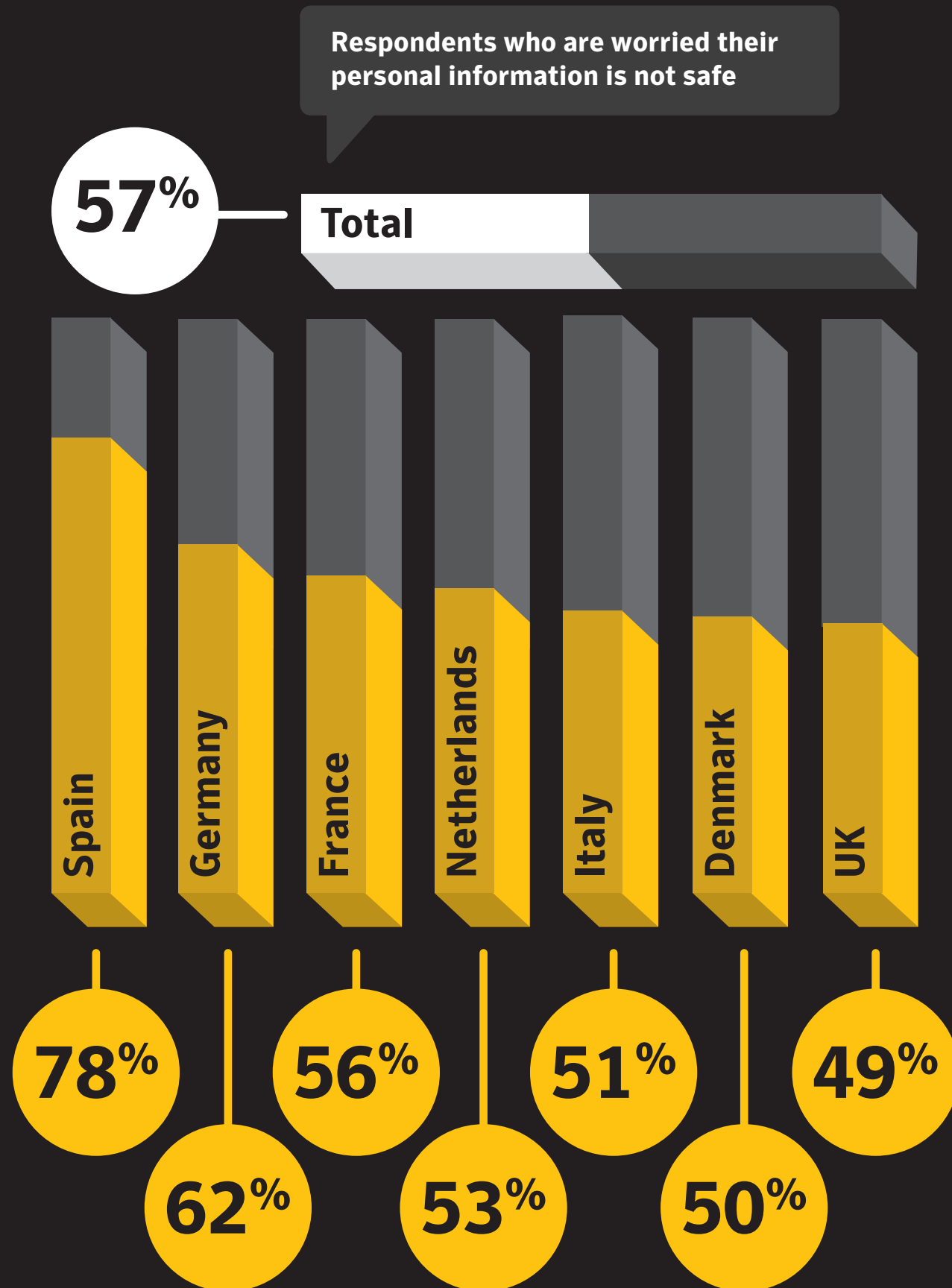
The average European is not happy with the way their data is handled by the companies they do business with.

Respondents also stated that their security concerns may cause a change in their online behaviours, as they choose to avoid certain services or activities online. This is likely to place pressure on businesses to adopt new practices. When business models rely on personal data, privacy and security features must be promoted.

“There is now a level of uncertainty regarding data. People are beginning to express their mistrust in businesses, particularly in the technology space.”

**Siân John**  
chief strategist for  
EMEA at Symantec





## Protecting data is a primary concern

**57%**

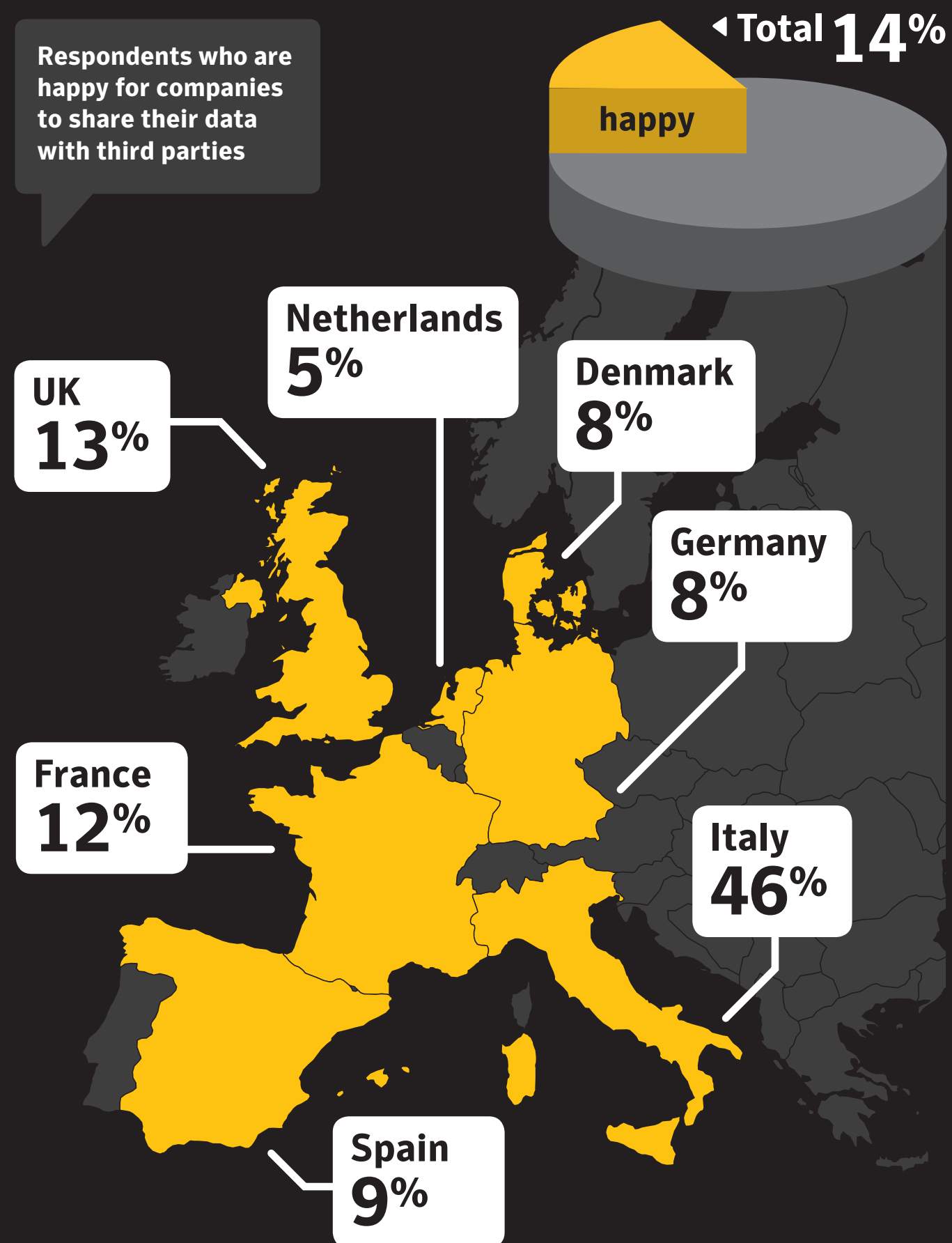
of Europeans are worried their data is not safe. This is of biggest concern to respondents in Spain, where 78% of people do not think it is safe. Germany was the second highest with 62% and UK-based respondents showed least concern at 49%.



**59%**

of respondents have experienced a data protection issue in the past. These issues include an email account being hacked, bank details stolen, online identity theft, a computer virus, social media account hack, responding to an online scam or fake email or been notified of a data breach by a company that I use.





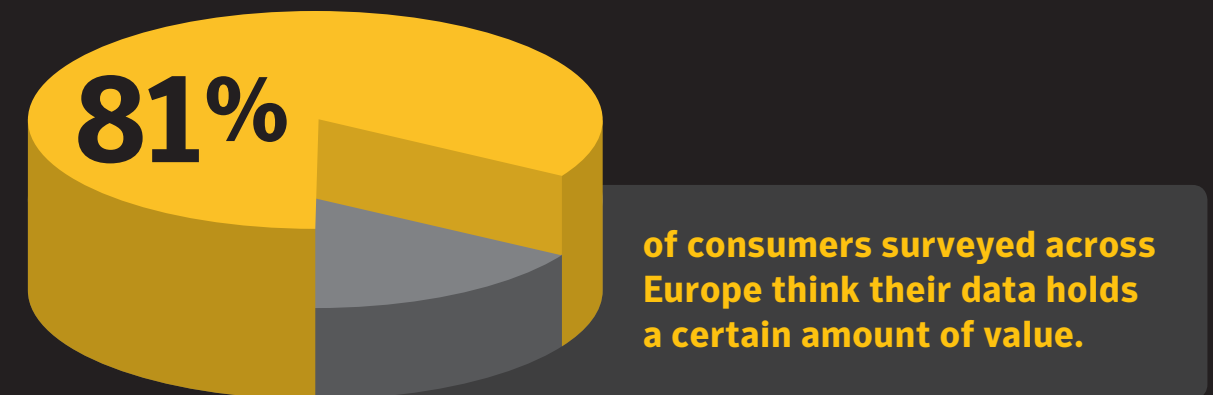
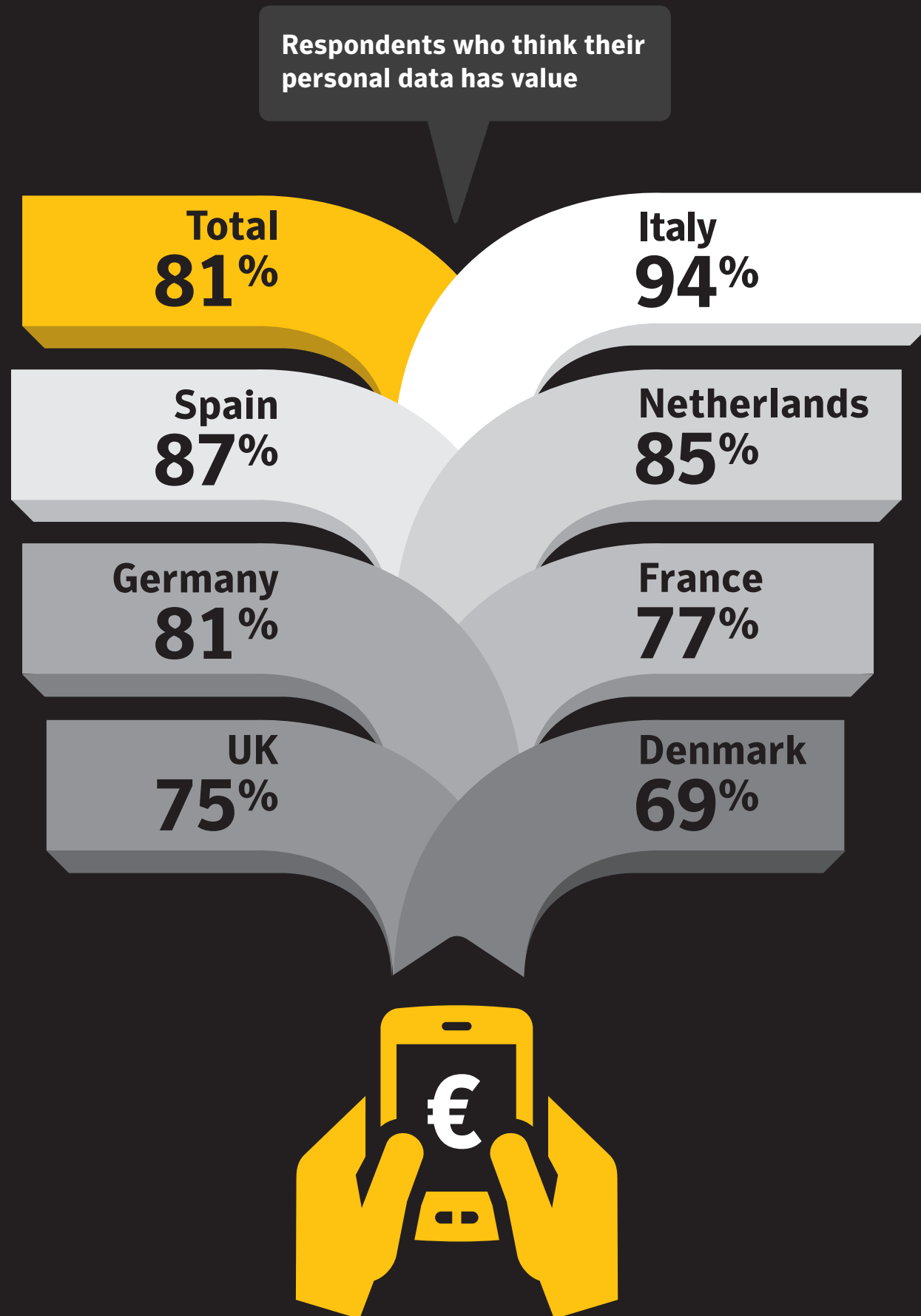
Companies, as part of their customer data collection policies, can offer to share customer data with selected third parties. When questioned on this practice, only 14% of respondents stated they were happy to share their data with third parties, with 47% being unhappy to share any data and 35% requiring some form of check on exactly what data was shared.



The results were broadly similar across all seven countries, apart from Italy where a significantly higher 46% of respondents were happy for their data to be shared with third parties.

The Italians differed to the European average on more than one occasion. They were the country with the highest percentage of people reading terms and conditions, so perhaps are well educated on what exactly they are signing up to. This level of maturity shows informed consent.

For many businesses, the opportunity to share customer data with third parties can be valuable, in terms of developing stronger customer relationships and providing better service. For those businesses, Symantec recommends they examine what they can do to improve customer trust that data shared will remain secure and private.



Consumers acknowledge their data can enable businesses to make money. Italians are most aware of that fact, with 94% thinking their data holds value.

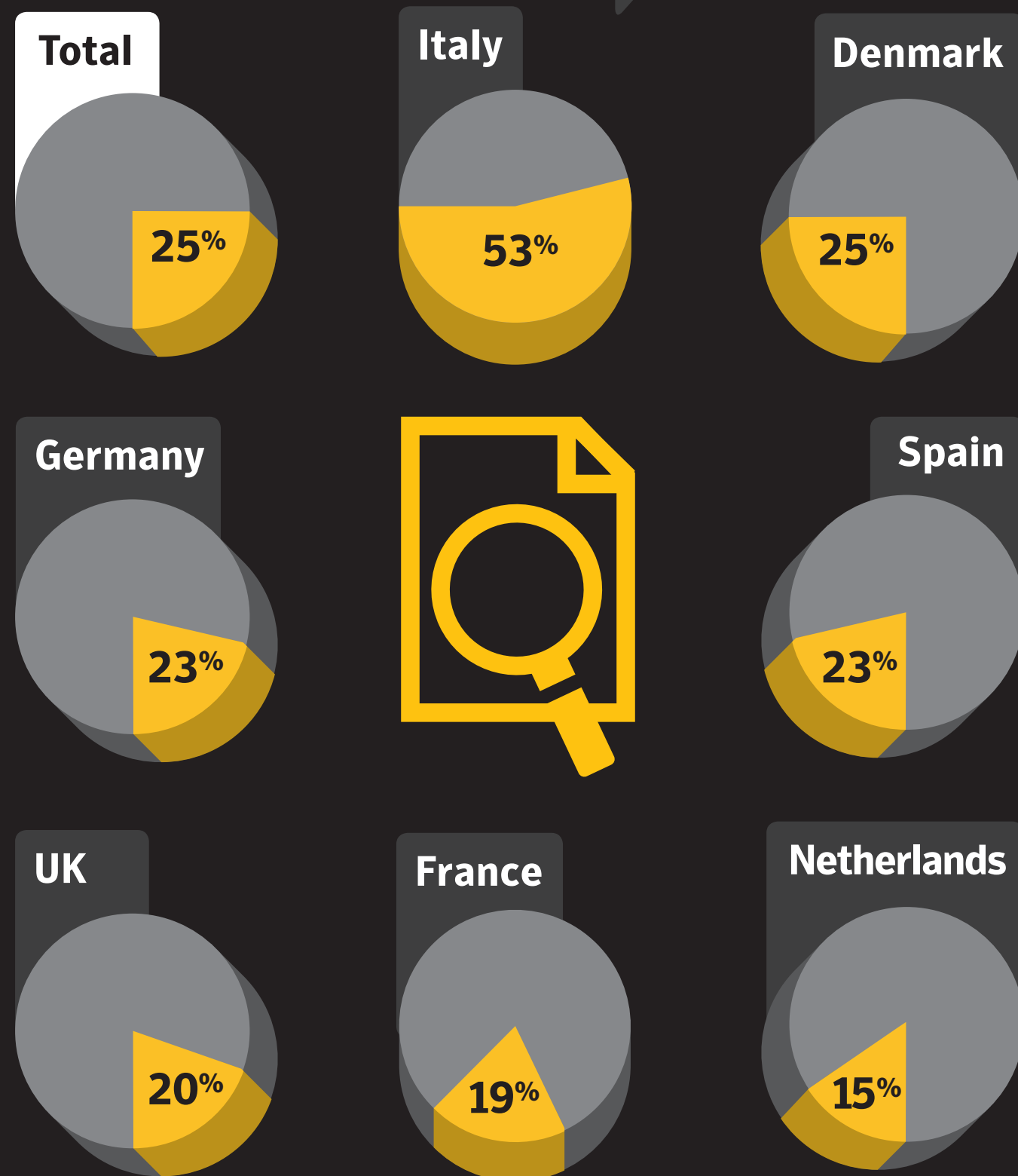
“For some years, we have predicted that the value of data will start to be understood by the creators of it. The State of Privacy report shows that many Europeans are starting to think about how their data might have significant worth to others. We have reached the tipping point.”

**Darren Thomson**  
CTO and VP of technology  
EMEA Symantec

Businesses may be surprised by how highly their customers value their own personal data.

Europeans place significant value on their data. When asked how much their online footprint is worth, **24%** think that it could be valued at €10,000 or more

Respondents who read the terms and conditions when they buy products or services online



Despite concerns over privacy and a high valuation of data, the behaviour of many Europeans is not reflected by their actions towards data protection.



Consumers are less cautious in their online approach, with only 1 in 4 people reading the terms and conditions in full when buying or signing up to products and services online.

**59%** of respondents confess to merely skimming the terms and conditions when making a purchase, while 14% state that they never read the terms and conditions.

In the Netherlands, only **15%** of people read the terms and conditions in full, which is significantly lower than Italy, where over half say they do.



“Terms and conditions for online services and products are in many cases hidden, long and difficult to understand or even misleading.

We recommend that companies and public sector bodies review their privacy policies and create simple, more effective methods of communicating these to consumers.

Better placement on the website, or as a more integral part of the customer’s journey are just two options to improve the customer experience.

We believe that terms and conditions should be more concise, easy to understand and companies should help customers take control of their data.”



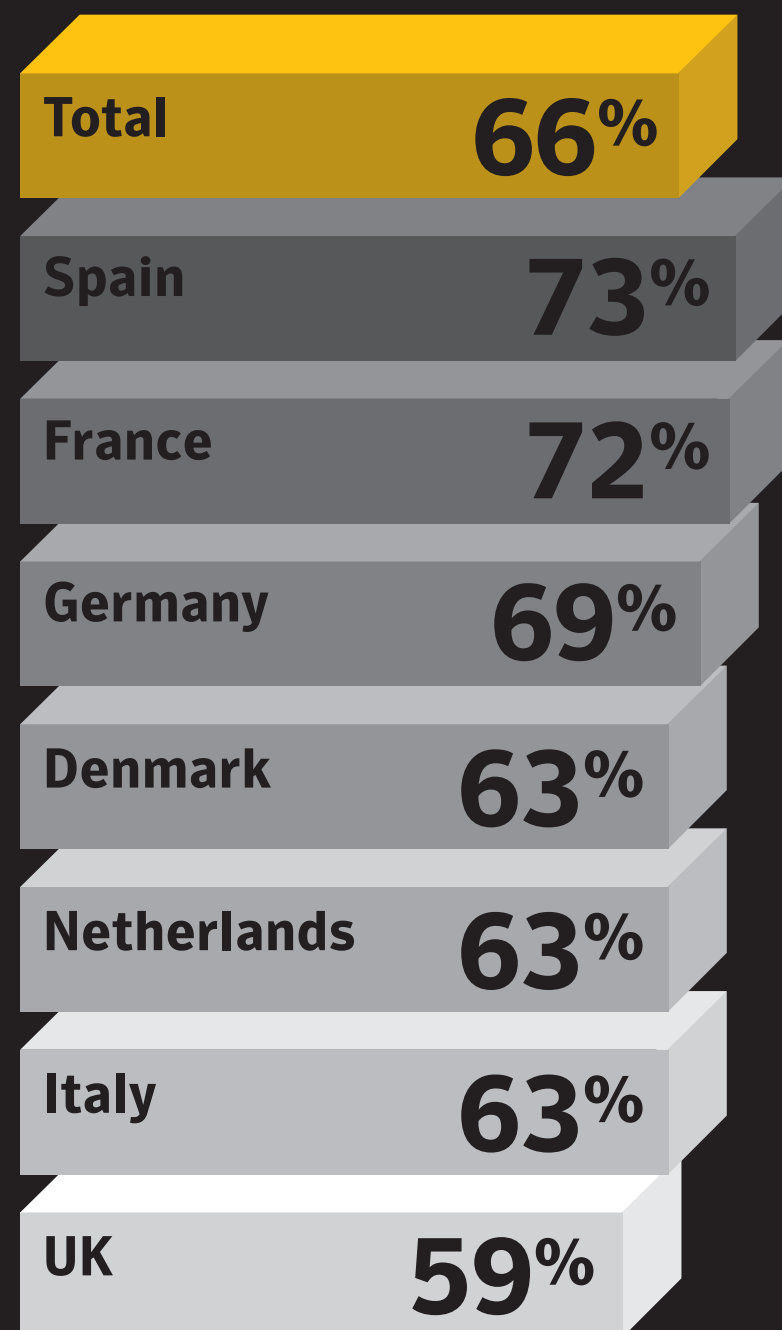
Professor Udo Helmbrecht  
executive director of ENISA

This situation presents an education opportunity for organisations. By adopting best practices for terms and conditions and privacy policies, companies will be better placed in the long term with credible information on their databases, in addition to building trust among customers.

Terms and conditions are one tool available to consumers to help them understand what they are buying or signing up to, yet not everyone is reading them.

**Despite much concern about the security and privacy of data, many are unsure what to do to better protect their data.**

Respondents who would like to better protect their personal details but are not sure how to go about doing this



One of the biggest issues that a consumer faces is how to act on a problem they may have with a particular term or condition, and where to go next if they have a data protection issue.

66% of Europeans are unsure what steps to take to protect personal information. This includes their personal bank details and their email addresses.

There is a need for both businesses and the public sector to do more to educate consumers on best practices to protect personal information.

There is an added requirement for businesses to promote better practices in their attitudes towards data. Over a third of Europeans are concerned that too many people have access to their personal details.

This feeling resonates highest with 73% of Spanish respondents. Despite this, Spanish consumers still use the services, but with only 23% in Spain reading the terms and conditions in full where they may discover further details about what access they are giving.

Concern over data safety is one issue, but when consumers are faced with a data security infringement, only 20% of people were confident that the issue would be resolved.



"Data breach notification informs and empowers consumers. It provides a transparency mechanism to show how data is effectively secured. When the GDPR is adopted we hope this transparency mechanism will give to consumers more confidence in the way industry and government protect their data."

Ilias Chantzios senior director government affairs EMEA at Symantec

# The Data Trust Gap

02

**The State of Privacy research uncovered a “trust gap” between organisations and their customers. This is the difference in how private a piece of data is perceived as being, and how securely people trust that it is held.**

By accessing and analysing customer information, businesses provide a tailor-made approach, examining behavioural trends and ultimately improving the customer experience. Analysis of anonymised data, such as medical information, has the potential to deliver huge benefit to society.

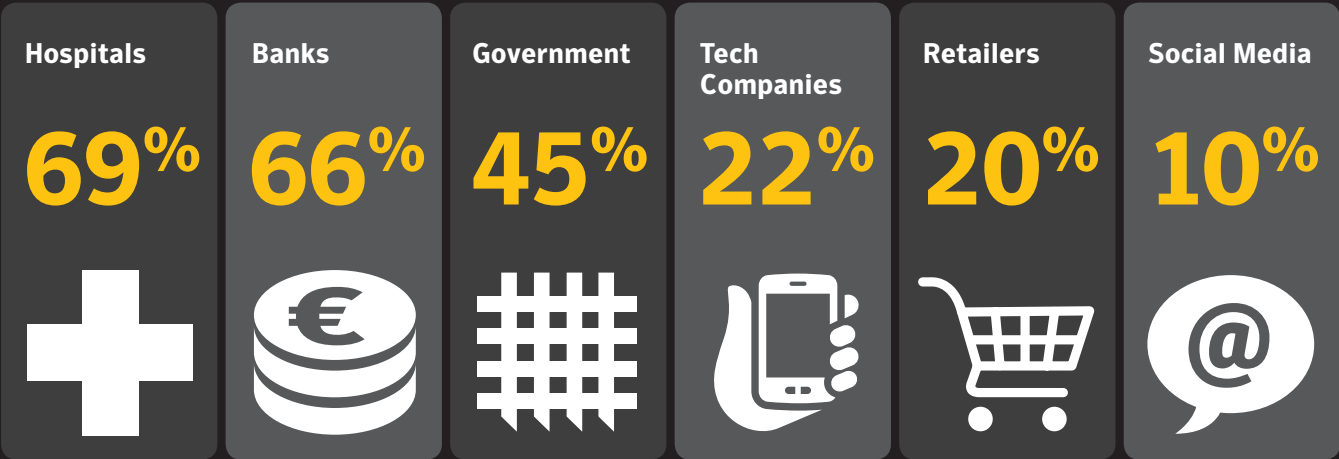
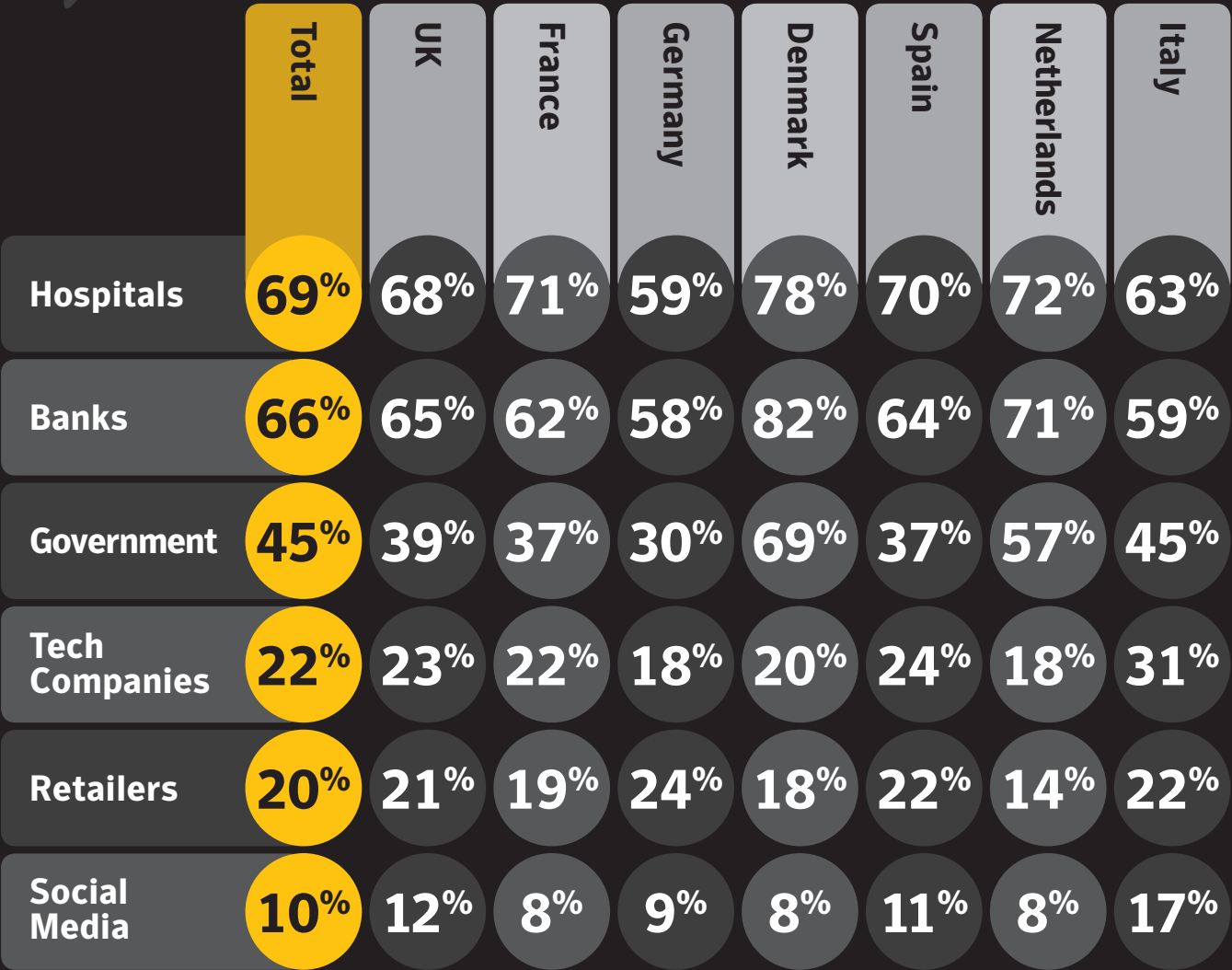
Without access to internet traffic data, which includes vast amounts of anonymous, pseudonymous, or even occasionally personal data, we at Symantec would not be able to analyse it, discover threats and protect our customers. It is fundamental to the privacy and security of data that resides with people, business and public authorities that we are able to access and analyse such data from the internet.

The trust gap exists due to consumers' concerns over the security of the data they have already shared. We are at a tipping point where organisations can take control of this issue and demonstrate their commitment to privacy, curbing this disconnect with the public and consumers.

**“Businesses should consider a channel to allow consumers to question how their data is being used and advocate more transparency. If businesses begin to act like trusted advisors and put the privacy of consumer data at the heart of the business, the consumer is on a much better footing to feel more confident about their data.”**

**Philip Carter**  
VP for European  
enterprise infrastructure  
and software group at IDC

Trust in the following organisations to keep data completely secure



The State of Privacy research showed the most trusted organisations are those that do not have an overt business model built on collecting data.

Of the 6 main sectors included in the study the least trusted organisations are retailers and social media, with only 20% and 10% respectively. Symantec sees the lack of trust in these companies as a reputational issue, possibly stemming from recent high profile data protection incidents.

Tech companies which have also suffered from recent data breaches, generated trust from only 22% of respondents

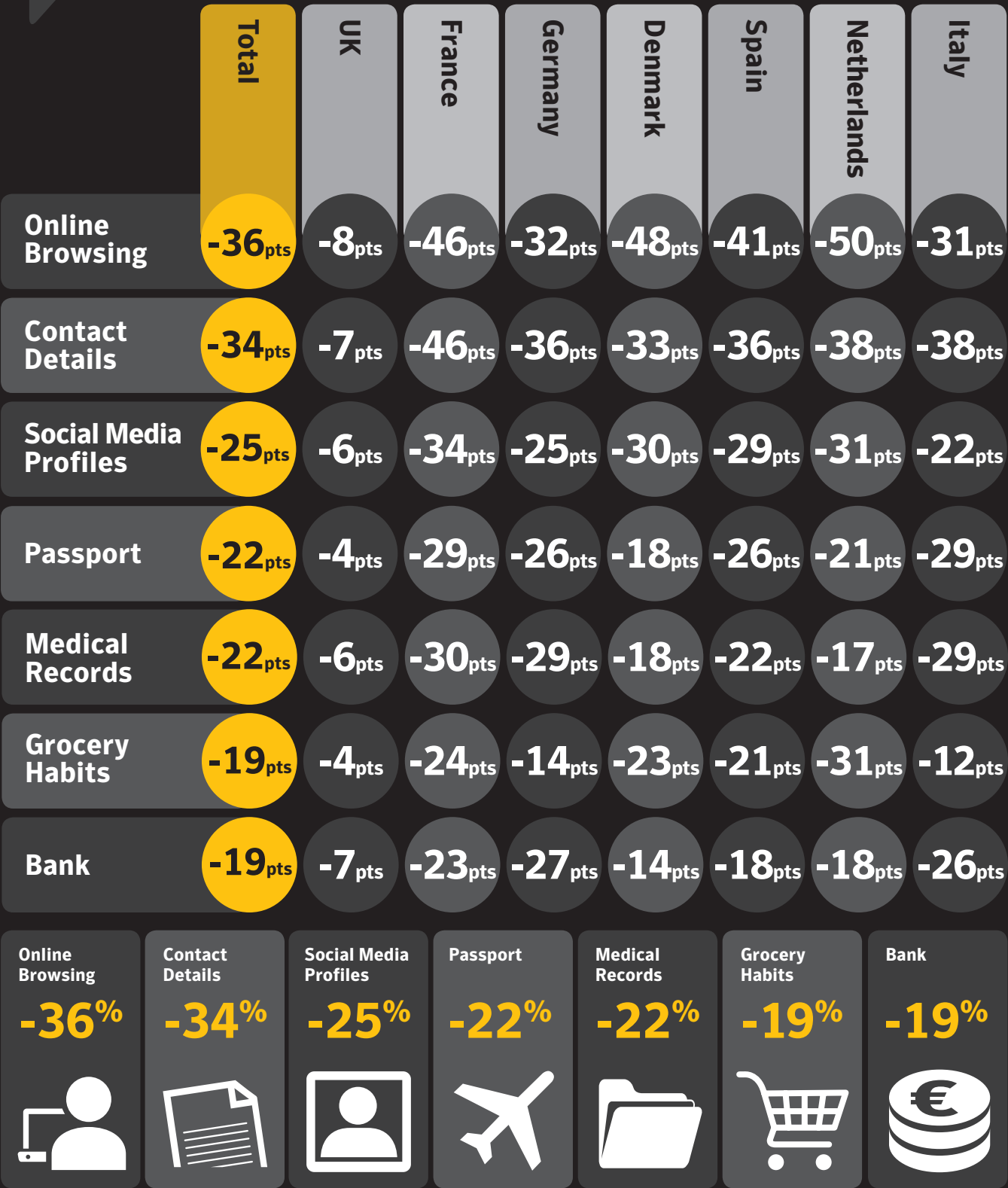


The most trusted sector was the health industry with a 69% level of trust. This is interesting when one examines the quantity of data breaches in this sector. Symantec’s Internet Security Threat Report indicated that health records are globally the fifth most breached type of personal data, and that the public sector is most at risk of targeted attacks.

“Consumer perceptions are really interesting here. We see a trend where those industry sectors gathering data for consumer protection purposes such as the medical industry or passport offices, have a higher level of trust. However, where companies’ business models are based on data – whether for web search or classification or social sharing – trust is much lower, and this is something which companies will need to address.”

**Siân John**  
chief strategist for  
EMEA at Symantec

Perceived privacy of data vs perceived security – The “Trust Gap”



The largest trust gap exists for online browsing, where there is a 36% difference between how private individuals believe their search history should be, and how secure they believe it is. A gap also exists in all other personal information sets. Even with vital passport information that is controlled by the government, the trust gap remains high at 22%.

“Businesses need to be more transparent with customers on how they are keeping data secure. Security needs to be embedded into a company’s value chain, but it should also be viewed internally as a customer winning requirement, and not just a cost.”

Ilias Chantzos senior director government affairs EMEA at Symantec

The trust in organisations is further undermined by concern over how companies profit from personal information.

We have already discussed how the report shows that Europeans think their data has transactional and financial value. However, the research also shows that the majority think companies are using their data to make extra profit.

- 32% believe personal data is being used to improve customer experience.
- 70% think their personal data is being sold on to third parties for profit.
- 74% of European respondents think it is unfair that companies are making money from their personal information.



These figures demonstrate the trade-off respondents are currently prepared to make, and show how convenience wins over security in today's society.

Across Europe, people consistently showed that they were prepared to divulge personal information, if there is an option to trade it for a benefit.

A third of respondents are willing to give their email address in exchange for a store discount, while 3 in 10 would be happy to do so for a chance to win a prize. While this remains true today, Symantec questions whether this will change if Europeans' trust in data privacy and security continues to be eroded.

However, benefits of data sharing outside of financial gain are not recognised.

“The report demonstrates we have not done enough to explain the societal benefits of big data. As a result we see consumers applying a short-sighted approach to data sharing, where they only share for direct and personal financial benefit. People are not willing to share because they do not think it is secure, they are concerned they will be identified from their data and worry about the potential impacts of that. We need to be providing a better view of how anonymisation and privacy enhancing technologies are used, how aggregated data are protected and what the broader societal benefits of data sharing are.”

Ilias Chantzos  
senior director  
government affairs  
EMEA at Symantec



## Where Does The Responsibility Lie?

03

**Government, business and consumers can all take different steps to ensure better data protection, and Symantec explored opinions on who is ultimately responsible.**

The responsibility in protecting information is relatively equal across government, business and consumers, according to the results. The majority (66%) of Europeans claimed they would be prepared to take steps to better protect their personal information, but stated they required help and guidance from external parties.

In fact, the research showed that consumers are willing to pay for data protection in the same way that they would pay for travel or credit card insurance.

“The law is favouring the introduction of new regulations to fill a gap left by those consumers that are not doing enough to protect themselves. Some parts of the economy are getting more attention than others and from time to time, we can expect mini explosions of consumer reaction.”

**Stewart Room**  
partner at PWC



Respondents who are willing  
to pay for data protection

**50%**

Would pay the same or more  
for data protection as their  
credit card insurance



**46%**

Would pay the same or  
more as their phone bill




“It is clear we are at a tipping point. It is now that business and government leaders should act to ensure their customers and the public can trust them sufficiently to share accurate data. The general public rightly believes the privacy and security of their data should be invested in. Data is fundamental to the development of business and society. The opportunities with data shared, analysed and used in a secure and private environment are endless. The data potential could revolutionise how we live today.”

**Darren Thomson**  
CTO and VP of  
technology  
EMEA Symantec





Percentage of responsibility governments, businesses and consumers should take in protecting personal information

	Government 	Business 	You 
Spain	44%	35%	22%
Italy	44%	33%	23%
France	37%	36%	27%
Netherlands	34%	22%	44%
UK	32%	28%	40%
Germany	32%	28%	40%
Denmark	32%	29%	38%
Total	36%	30%	33%

Governments were given the most responsibility overall for data protection at

36%

and citizens in France, Spain and Italy seemed to rely most heavily on them.

The responsibility of business ranked lowest at

30%

overall, while 33% put the responsibility to protect data with the individual.

Of the respondents who work with personal data, less than half of those surveyed believed that their employers enforced basic security processes, including frequent password changes (42%) or regular protection software updates (44%).

To promote better data privacy practices and processes within organisations, Symantec recommends that businesses:



**Analyse your own data: ensure you know what you have and what needs to be protected.**



**Embed security within your internal value chain, and your supply chain.**



**As you develop new products and services, take a customer-led approach, consider possible privacy implications.**



**Ensure your own systems are protected against data breach both internally and externally. In the event of a data breach communicate in a timely manner with all relevant audiences.**



**Regularly communicate with your customers on the best ways to keep their data secure.**



**Demonstrate to customers that their data is being used to improve services and propositions.**



**Promote data privacy education and guidance to your entire business – it should be part of the employee value proposition.**



**Front line customer services should be able to answer questions on data security and privacy.**



**Privacy policies and service terms and conditions should be easily accessible, succinct and clear to understand.**



**Provide customers with an identified data privacy point of contact within the organisation.**

“Treating consumers honestly and with respect, by providing clear and truthful information about privacy practices, is fundamental to generating trust and confidence.”

**Stewart Room**  
partner at PWC

# The Future of Data Privacy

04

**The State of Privacy research shows how important data protection is to the majority of Europeans. High profile data hacking and debates over government surveillance are exacerbating the issue.**

Europeans are more conscious of how they use the internet, where they use it, and what steps they can take as individuals to protect themselves against any threats.

The report explored whether Europeans will take a step back in regards to the data they give out. It showed that online self-moderation is prevalent as individuals claim they will post less, give out false information, or even reduce the amount of time they spend online.

“Customers will certainly migrate to those companies and services that they consider to be safest. In the future, I believe customers will move on from searching out the best deal to form “buying tribes” and leverage their knowledge to promote joint purchasing power from those businesses that they trust the most.”

**Peter Cochrane**  
scientist, engineer  
and entrepreneur  
at Cochrane  
Associates Ltd



Importance of factors when choosing a company to shop with or use

	Total	UK	France	Germany	Denmark	Spain	Netherlands	Italy
Keeping your data safe and secure	88%	89%	88%	86%	88%	87%	88%	88%
Quality products	86%	88%	86%	82%	86%	85%	86%	86%
Delivering great customer service	82%	85%	83%	76%	82%	83%	81%	85%
Treating their employees and suppliers fairly	69%	69%	67%	69%	60%	76%	73%	67%
Being environmentally friendly	56%	50%	55%	49%	45%	66%	52%	72%
Giving back to the community	47%	46%	50%	43%	30%	65%	43%	54%

Data security is very important to European consumers: 88% say this is important when choosing a company, more important than the quality of the product (86%) or the customer service (82%).

Keeping data safe and secure (88%) now also rates far ahead of environmental concerns (56%) for shoppers.

“The recent major breaches and the broader discussions about appropriate limits to government surveillance have put a spotlight on the question of privacy and how it impacts customers and the public at large. As a result there is a perception that industry is not doing enough to protect personal data, contributing to the trust gap. This perception has resulted in a much broader public debate about what industry and government are doing and highlighted a real public sensitivity. More is needed from industry and government to explain the positive contribution they are making.”

Ilias Chantzos senior director government affairs EMEA at Symantec

“Business must respect the user and gain trust. At Symantec we know that consumers will end transactions if a company has a poor data protection reputation. A high level of trust will ensure accurate data, this will allow businesses to not only make more money but the trends can be used to aid product development and guide the direction of the business. Companies should not pay lip service to data protection issues, but educate and inform users on data protection and privacy policies in a straightforward manner.”

Siân John chief strategist for EMEA at Symantec

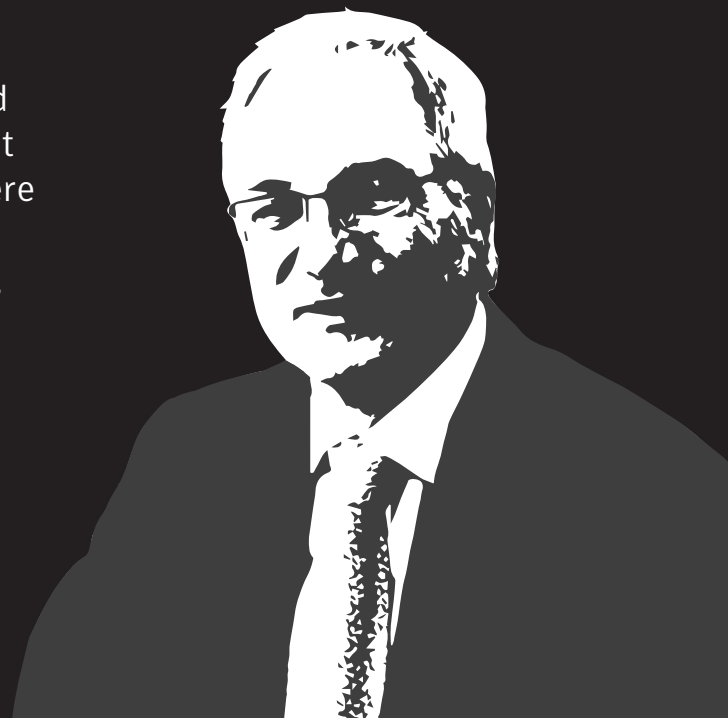


The old models for data security, a **castle and moat approach** to ring-fence valuable information, have become irrelevant with the advent of smartphones and tablets, cloud computing, social networking, and the emerging internet of things.

Connected devices and the internet of things all generate large quantities of data. There are significant benefits to business in being able to correlate and analyse large amounts of this data, but this data must be kept secure, and there must be trust among customers that their data, anonymised or identifiable, is secure.

“Awareness raising has a key role in enhancing the general public’s understanding of privacy issues and relevant mitigation measures.”

**Professor Udo Helmbrecht**  
executive director  
of ENISA



“Symantec believes that one of the major reasons that data privacy is becoming such a concern is because there is now a clear understanding amongst consumers that their data holds value. Providers of technology service should take heed. The IT industry is not trusted today to do the right thing by consumers when it comes to data privacy. Much work will need to be done in the coming years to build and sustain this level of trust.”

**Darren Thomson**  
CTO and VP of  
technology  
EMEA Symantec

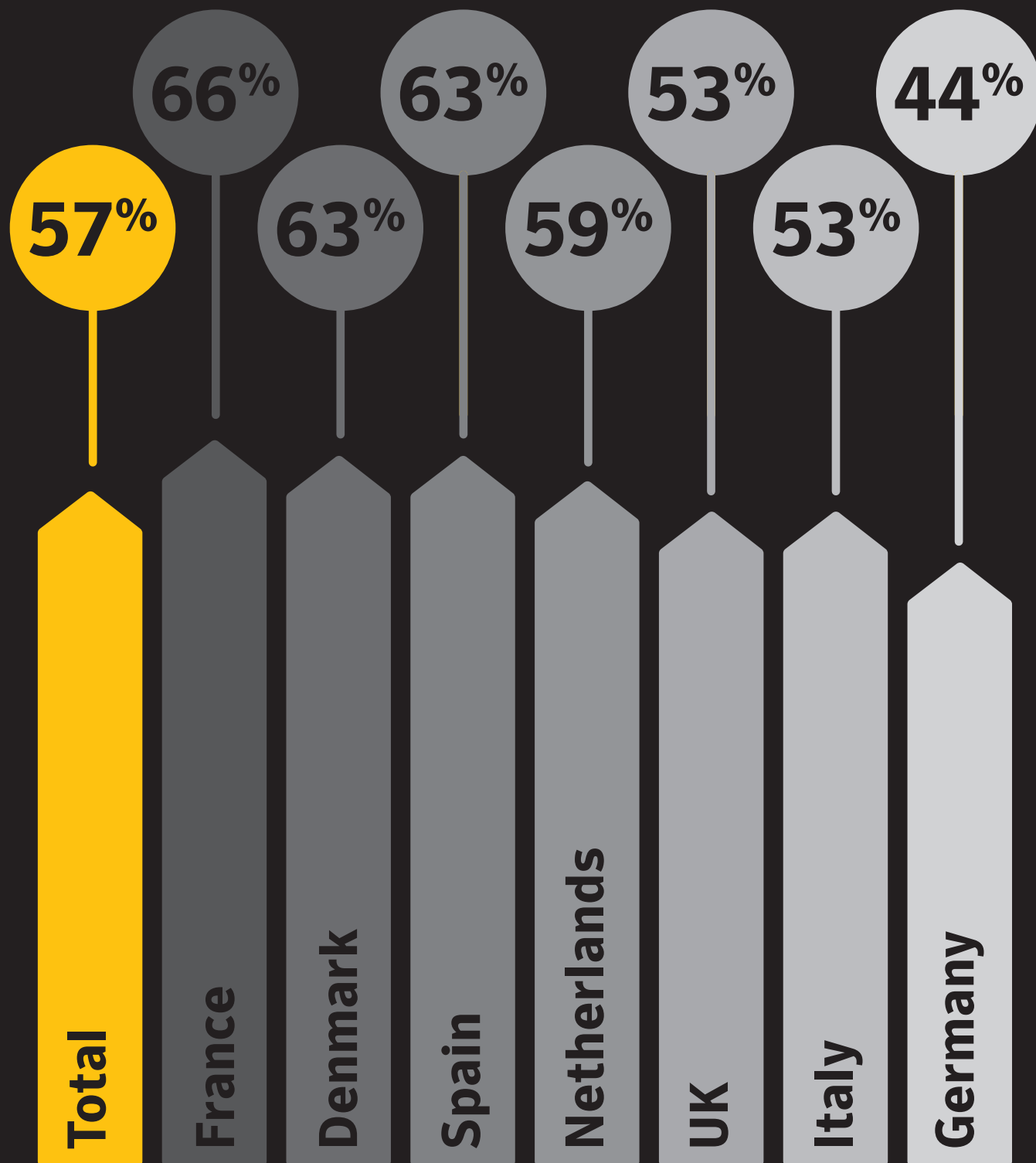


“It’s great to see the consensus across Europe on the importance of data protection. There is a real consistency emerging that privacy is a competitive advantage for businesses and that privacy concerns also determine consumers’ behaviour. It is critical to ensure consumers are empowered to understand what their data is being used for and how it is protected.”

**Ilias Chantzios**  
senior director  
government affairs  
EMEA at Symantec



### Respondents who would avoid posting personal details online



Europeans are actively adopting a self-moderation approach to their personal data and taking the matter in to their own hands. According to Symantec's research, over half of those surveyed (57%) are now avoiding posting personal details online.

As data concerns increase, Symantec's experts warn that individuals could avoid posting personal information online. As data is seen as a valuable commodity, it could ultimately have long term effects to the way we do business.

Another popular approach to self-moderation could also have chilling repercussions for business, as 1 in 3 consumers admitted they provide false information in order to protect their privacy. 36% of Germans and 34% of UK respondents stated they had given fake details online, in a bid to avoid giving out their credentials, which will be equally worrying for businesses basing programmes, projects and campaigns around this data.

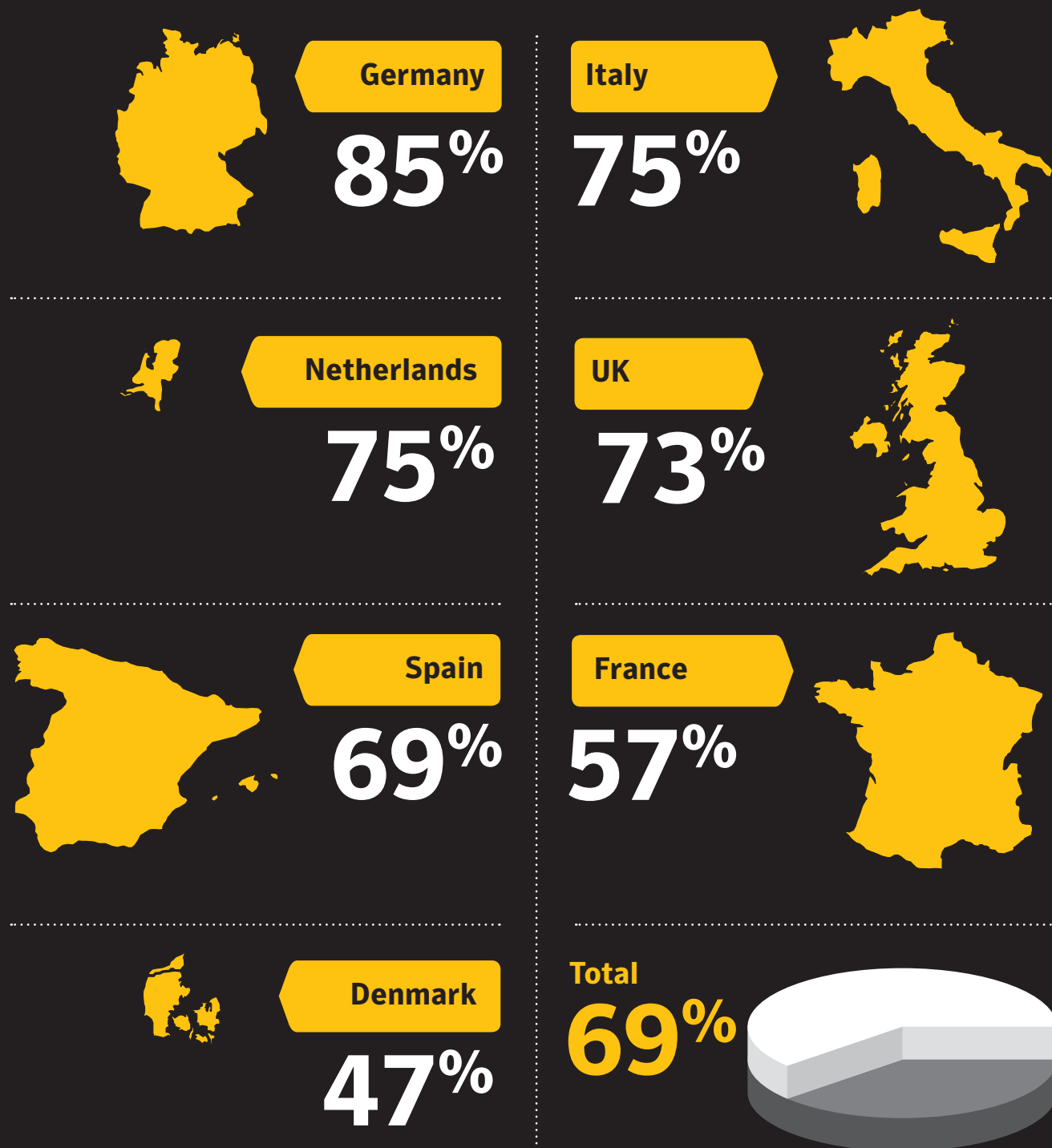
"If you're a business relying on user data, take heed of this information regarding false data from consumers. You may be putting your faith in user data at the expense of truth. Data does not always acknowledge the human side of your customer. Too much reliance may deliver an advertising or marketing campaign with little relevance."



**Siân John**  
chief strategist for  
EMEA at Symantec



Respondents who would take a break from the internet



People are now considering avoiding the internet altogether, as the most extreme example of self-moderation. Two thirds of respondents said they would take a break from the internet in order to protect their data.

“As with the adoption of all technology, security and privacy can be left by the wayside in the rush to achieve financial growth or obtain a product or service in a fast and convenient manner. Errors have been made on both sides: businesses have learnt the hard way how to maintain data security and forge strong relationships with customers, while consumers are now beginning to vote with their feet and choose businesses and services who respect and maintain consumer security and privacy.”

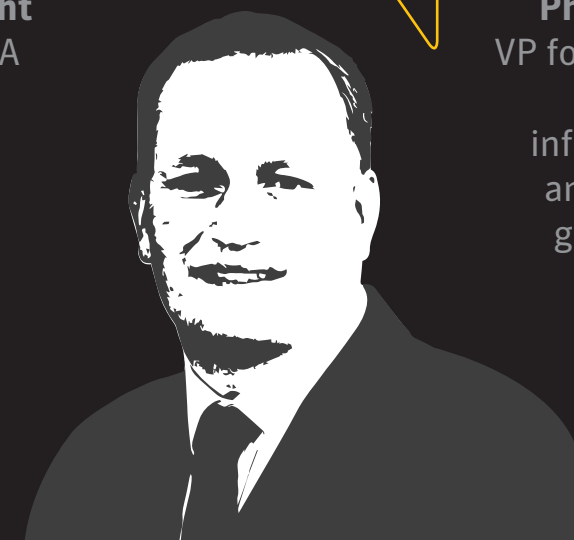
**Siân John** chief strategist  
for EMEA at Symantec

“Governments can help reduce the trust gap between businesses and users by making the former accountable for data protection and by strongly enforcing compliance with the underlying legal obligations.”

**Professor Udo Helmbrecht**  
executive director of ENISA

“I do think people will boycott certain businesses if the abuse goes too far and people begin to understand the practices behind the use of data. People are increasingly concerned about their digital footprint and considering how it might affect them in the future. The trust gap is real, there is now no question about it.”

**Philip Carter**  
VP for European  
enterprise  
infrastructure  
and software  
group at IDC



# Biographies



**Darren Thomson,**  
CTO and VP of technology,  
EMEA, Symantec

Darren is responsible for creating and leading marketing strategy across the EMEA region. Since joining Symantec in July, 2003, Darren has run various groups including global services practices covering Business Continuity Management, Storage & Data Management and Cloud Computing.



**Dr Peter Cochrane,**  
scientist, engineer and entrepreneur,  
Cochrane Associates Ltd

Peter is a futurist, entrepreneur, business and engineering advisor to international industries and governments. With over 40 years of technology and operational experience, Peter has been involved in the creation and transformation of corporations.



**Ilias Chantzios,**  
senior director, government affairs  
EMEA, Symantec

Ilias represents Symantec before government bodies, national authorities and international organisations advising on public policy issues with particular regard to privacy, data protection, IT security and data risk management and availability.



**Philip Carter,**  
vice president, European enterprise,  
infrastructure and software group, IDC

Philip leads a team of analysts that cover the infrastructure, middleware, and applications software markets and is tasked with writing and presenting on broader enterprise infrastructure software trends and the impact of emerging technology areas such as Big Data, cloud, mobility, and social as they relate to the European region.



**Siân John,**  
chief strategist for EMEA  
at Symantec

Siân leads articulation around Symantec's overall technology strategy. She has a particular focus on cyber and information security. Siân has worked in the IT industry for over 20 years, both as a security architect and as an independent security consultant.



**Professor Udo Helmbrecht,**  
executive director, European Union Agency for  
Network and Information Security (ENISA)

Professor Udo is the Executive Director of ENISA, a role he has held since October 2009. His experience in the field of security has been acquired through extensive work in a variety of areas, including energy, insurance, engineering, aviation, defence, and the space industry.



**Stewart Room,**  
global head of cyber security and  
data protection law at PwC Legal

Stewart advises companies on their strategies for using personal data and confidential information and on how to handle serious security breaches. With over 20 years of experience as a barrister and solicitor, Stewart specialises in privacy, data protection and data security law.





[www.symantec.com](http://www.symantec.com)