The Positive Way

WAVESTONE

PROTECTING PRIVACY IN THE DIGITAL AGE

FROM BIG DATA TO SMART DATA

The Positive Way

WAVESTONE

www.wavestone.com

In a world where knowing how to drive transformation is the key to success, Wavestone's mission is to inform and guide large companies and organizations in their most critical transformations, with the ambition of a positive outcome for all stakeholders.

Today's hyper-connected world—and the associated emergence of new technologies like data mining, connected objects, and artificial intelligence—is driving **a genuine data revolution**. More than ever, it's data that is providing the levers for digital transformation—**and capitalizing on it is rapidly becoming a strategic priority for organizations.**

Until now, their preferred approach has been the mass, and systematic, harvesting of personal data. Through this, organizations have built large databases that capitalize on the entirety of the "connected ecosystem"—both its personal and professional sides! But recently, the regulatory landscape has shifted in terms of privacy. The result has been a new and unprecedented level of awareness among people about the issue, and an emerging crisis of confidence —a risk that organizations would do well to address.

The writing is on the wall: after years of passive acceptance, people want to take back control of their data and digital privacy.

One thing is clear though: **there can be no data revolution without trust**. For organizations, lost trust places the adoption of their new digital offerings at risk—a real competitive disadvantage. They need to adapt, and ask themselves some searching questions: how can we reconcile the value offered by data, respect for people's privacy, and regulatory compliance? **How can we move from a big-data to a smart-data approach?** A balance clearly needs to be struck. Some will see the current situation as an opportunity, a chance, for example, to make a strength of data privacy. **And what about you? How will you capitalize on this coming revolution? What new uses will you develop—and how?**

GÉRÔME BILLOIS- Partner

AUTHORS

Raphaël BRUN

Raphaël is a Senior Manager in Wavestone's Cybersecurity & Digital Trust Practice. He brings expertise from a number of years of solid experience in the field of personal data protection. Raphaël manages compliance programs on behalf of clients across a range of sectors (retail, transport, insurance, etc.) and supports the regulatory compliance aspects of a number of public-sector projects (on health data recovery, transport fraud, etc.). He has also worked on the design of cybersecurity crisis management processes and on running crisis simulation exercises.

raphael.brun@wavestone.com

Damien LACHIVER

Damien is a Manager in Wavestone's Cybersecurity & Digital Trust Practice with expertise in data protection and cybersecurity crisis management. In particular, he manages compliance programs on behalf of clients for the EU's GDPR regulation and facilitates cybersecurity crisis simulation exercises.

damien.lachiver@wavestone.com

Adèle COUDERT

Adèle is a consultant in the Financial Services Practice. She is involved in numerous personal data protection projects and GDPR compliance programs.

adele.coudert@wavestone.com

Débora DI GIACOMO

Débora is a Senior Manager in Wavestone's European Services team. Débora has solid experience in IT strategy, business, and research consulting—with a focus on European Institutions. The main areas she consults on are digital government, interoperability, impact assessments of European policies, cost-benefit analysis, and technical feasibility studies.

debora.digiacomo@wavestone.com

Anaïs ETIENNE

Anaïs is a consultant in the Cybersecurity & Digital Trust Practice. Through her consulting experience, in particular on GDPR compliance programs for major players, she has developed expertise in personal data protection and risk management.

anais.etienne@wavestone.com

We would like to thank Gwendal Le Grand, Tristan Nitot and Benjamin André for providing us with three interviews to enhance this publication. We also thank Pascal Vidal and Nick Prescot for their contribution, as well as all the Wavestone consultants whose feedback has made the production of this document possible.

SUMMARY

THE PUBLIC ON HIGH ALERT WHEN IT COMES TO PROTECTING DIGITAL PRIVACY

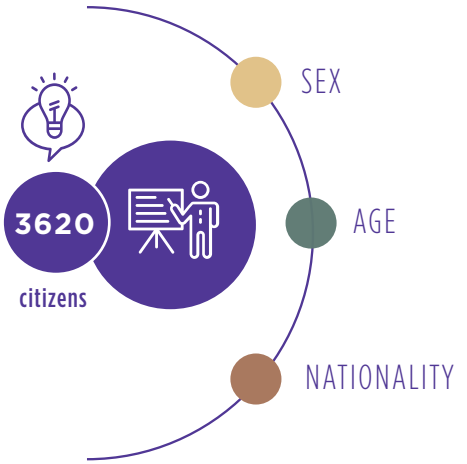
A SECOND INTERNATIONAL SURVEY

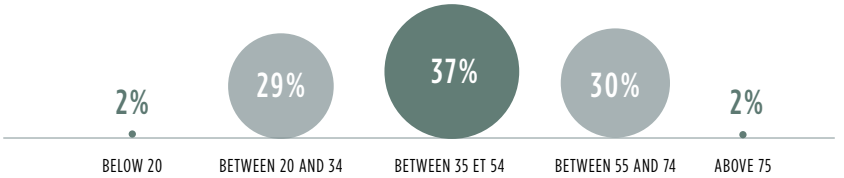
Wavestone regularly conducts public surveys to assess trends in digital privacy.

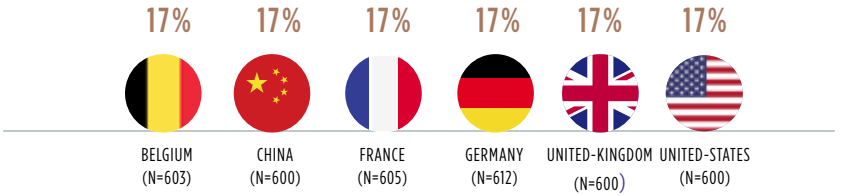
The results of our initial survey were published in 2016 in «Privacy in the Digital Age.» The findings of that study were further explored in a second survey, conducted in October 2018. This enabled us to measure the impact of the GDPR's entry into force on people's sensitivity to digital privacy.

The survey had 3,620 participants from six countries around the world. Participants were drawn from Belgium, China, France, Germany, the UK, and the US. These countries were carefully selected to test possible differences in perceptions about digital privacy that might arise from different countries' socio-economic statuses and national regulatory frameworks. Study participants were evenly distributed in terms of gender and age group. As a result, there was no over-representation of the 20 to 34 age group, which tends to have a greater sensitivity to privacy issues.

General statistics







AN UNPRECEDENTED INCREASE IN CONCERN AMONG PEOPLE

Concern is rising among people, on a global scale

94% of respondents say they are **concerned about privacy—an increase of 19% in two years**

An unprecedented increase in levels of concern! The results of our survey suggest **that people across the globe, not just in Europe**, **are increasingly concerned about their privacy**—and that their expectations, as a result, **are broadly similar**. In fact, we found that there was little or no difference between results from different countries. This sensitivity about privacy is gaining momentum year-on-year and is likely to be a long-term issue, something driven, in particular, by the tightening and broadening of the regulatory framework.

For most people, privacy issues are linked—above all—to being in control of their digital lives

2/3 For two thirds of people, **"privacy" means "online privacy"**

In our 2016 study, we highlighted the changing meaning of «privacy» as the digital revolution continues. Historically, privacy issues have been closely linked to freedom: people's freedom to maintain a degree of anonymity in their activities and to be able to isolate themselves to protect their interests. Today, faced with personal data, in all its forms, being gathered in ever-increasing volumes, people clearly **associate the protection of their privacy with having control of their data.**

As in 2016, people primarily defined privacy as being about controlling «who gets information about me.»

Even before the questions of knowing what data is being collected and what it's being used for**, people primarily associate data protection with the ability to choose which third parties can collect and process their information**

Ultimately, people are willing to share their personal data with others, but at a price—that of trust.

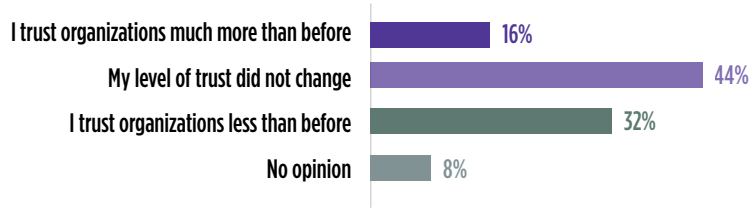
TRUST IN THIRD PARTIES IS DECLINING...

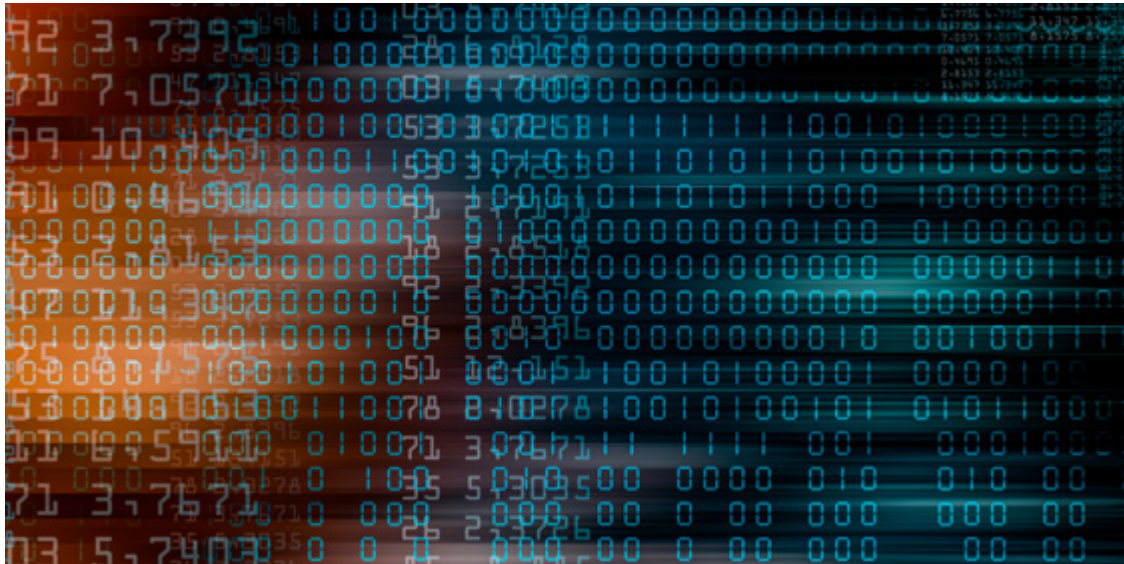
A general decline in the degree to which third parties are trusted

This decline can be easily explained by the increasing number of data breaches, or at the very least by the media interest they generate, something that was clearly the case for the Facebook/Cambridge Analytica and Equifax scandals.

32% of people report that **their level of trust in third parties on privacy protection has decreased over the last year**

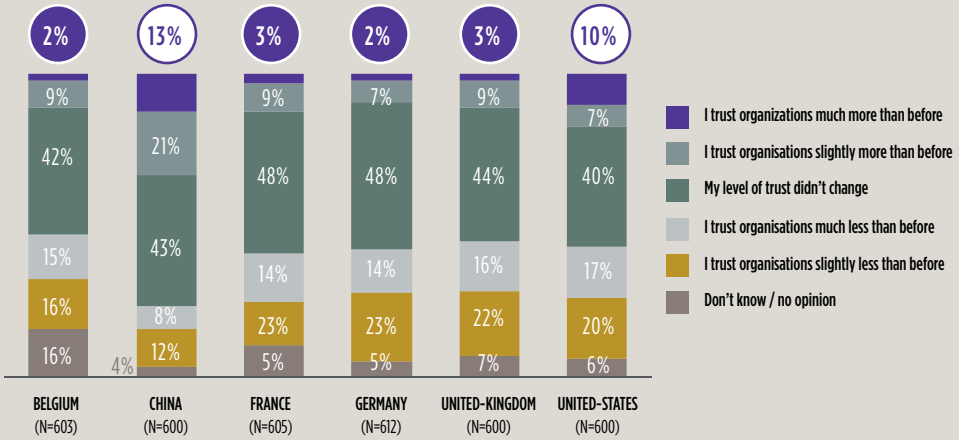
Do you feel that your trust in organizations has changed over the last year, regarding their use of your data?





The GDPR has provoked a crisis of confidence in Europe!
As a result of the regulation's own complexity, leaks that have been well publicized, and the scandals associated with them, people are increasingly wary.

Do you feel that your trust in organizations has changed over the last year, regarding their use of your data?



Our study shows a particularly striking set of results for European countries. Despite the entry into force of the GDPR (a regulation designed to rebuild trust) and the efforts made by organizations to comply with it, 68% of European respondents say they have not noticed any change with respect to the control of their data. Worse, comparing the results with the 2016 survey, some clearly feel they have even less control.

This crisis of confidence reflects an increasing degree of awareness of the issues that surround data protection: people are more informed about it, in particular through media coverage of the GDPR and awareness-raising efforts by regulatory authorities or even their own organizations. The result may also reflect a **misunderstanding of what organizations are doing in this area**, or a growing mistrust of what people see as a «black-box» approach to processing their data. The small number of campaigns aimed at consent renewal, and various communications around the GDPR, have not proved enough; and understandably so—trust takes time to build.

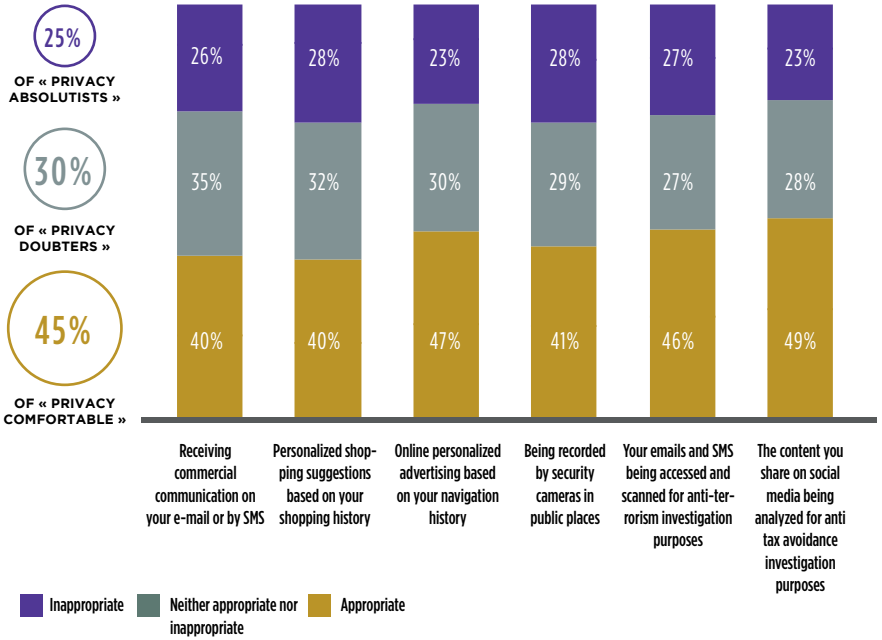
A quarter of people are «privacy absolutists»: regardless of how their data is used, they don't approve of it

Another finding from our survey is that the proportion of respondents who are willing or unwilling to share their data varies only very slightly with the reason why the data is being collected. This suggests that how the data is being used is not the central issue for most people. Analysis of the survey results (shown in graph below) clearly distinguishes these three types of attitude toward data.

- **45% of the population can be described as being «privacy comfortable».** They don't mind sharing their data. People in this category didn't need to wait for the GDPR's entry into force, or reassuring communications from the relevant organizations, before accepting new digital uses and sharing their data as the quid pro quo for access to them.
- **30% of the population can be described as being «privacy doubters».** People in this category understand the interest in sharing their data in order to access a service. However, they need a clear framework to be able to trust the third party that they will have to share the data with. GDPR compliance, along with clear, transparent communication, can provide such a framework—and persuade these people to share their information.
- **25% of the population can be described as being «privacy absolutists».** People here are especially reluctant to share their data. Unlike those in the previous category, regulatory compliance won't be enough to persuade them to part with personal information. For them, there's a need to find other ways to build trust. The real

challenge for organizations is to limit an expansion in the size of this third category, or even to identify levers that will persuade people to buy into digital services requiring the provision of data. Possible ways to do this are discussed in the third part of this publication.

Please evaluate the appropriateness of the use of your personal data in the following situations:



A persistent irritant: unwanted commercial solicitations

1/3 of our respondents said that **they have asked an organization to stop sending them communications**

Despite the general lack of interest in how collected data is used, one use nevertheless continues to be an irritant: unwanted commercial solicitations. Historically, marketing teams have tended to collect as much contact data as possible—to give themselves the best chance of sending the right email to the right person. However, this practice has a serious consequence: the guaranteed annoyance of those individuals who are repeatedly solicited.

This is reflected very concretely in the survey results: a third of our respondents said that they have asked an organization to stop sending them communications, a request that is also the most frequently used data-related right. France's regulatory authority confirms this, indicating that 21% of the complaints it receives are related to commercial prospecting—with a significant increase in complaints relating to solicitations via SMS. **Seen from an individual's point of view, this ill-advised over-solicitation directly degrades levels of trust with the third party—which is identified as its most important consequence by our respondents.**

There is, therefore, a real challenge—one that involves creating qualitative marketing databases not built solely on a person's general interest in the area that the communication relates to. By investing in digital privacy, organizations can achieve **more personalized and effective marketing**. The systematic collection of clear, informed consent, as set out in the GDPR, is a first step toward minimizing complaints and loss of trust. Going beyond this, organizations can refine the personalization of commercial relations still further; for example, by requesting consent even when the GDPR does not require it, or by allowing the exertion of this «relational pressure» at a more granular level. Doing this offers an effective way to maintain or develop trust. The idea is to genuinely engage people and establish a dialogue that builds relations over time.

...WHICH MANIFESTS ITSELF IN PEOPLE TAKING A MORE OFFENSIVE STANCE TO PROTECT THEIR PRIVACY

1/2 of respondents said **they have exercised their privacy-related rights in the past year**

Going beyond simply being aware of the issue, people are taking a more aggressive stance to protecting their privacy. They are no longer prepared to accept the intrusion of organizations into their private lives and, as a result, are much less likely to agree to the mass collection of personal data. To make up for years of accepting such a state of affairs, **some people have seized the initiative, seeking to take back control**

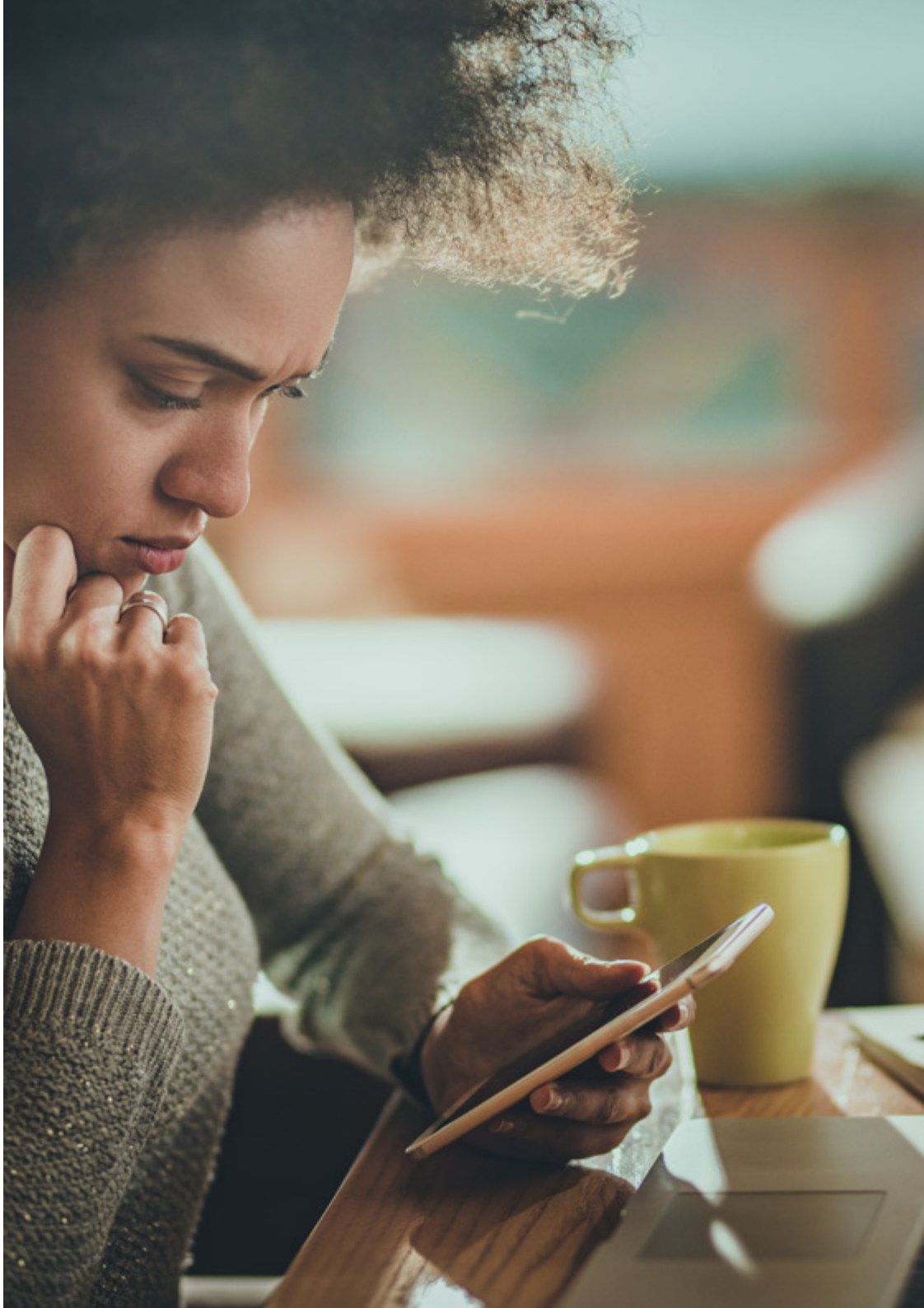
using the means now available to them—especially those provided by the GDPR. In concrete terms, they have no hesitation in using their rights, and **are even prepared to lodge collective complaints** when the regulatory framework allows it.

Faced with the prospect of their customer databases being depopulated, so far, only 15% of organizations have chosen to pursue consent renewal campaigns. As a result, people have taken advantage of strengthening regulations to spontaneously withdraw their agreement to certain types of data processing—or even to request the outright deletion of all their data. More than half of respondents said that they had exercised their privacy-related rights in the past year, a clear increase in requests, and something evident on the ground for organizations. When they are not satisfied with the response to their requests, in terms of time or quality, people no longer hesitate to turn to the authorities.

In order to increase impact and manage costs, consumers are working together to lodge collective complaints. They are supported by consumer associations (the best known being NOYB, Privacy International, and La Quadrature du Net) who position themselves as defenders of citizens' data rights. These associations have no hesitation in attacking digital giants like Google, Amazon, Facebook, LinkedIn, and others. To highlight excesses and raise awareness among the general public, Privacy International also organizes an annual competition—the Big Brother Awards—which highlights the worst infringements of people's privacy and freedoms.

> «In 2018, the CNIL (the French data protection authority) received a total of 11,077 complaints—an increase of 32% over the previous year.»
>
> *GWENDAL LE GRAND, Director of technology and innovation at CNIL (the French data protection authority)*

Clearly, **the public and consumer associations are starting to get to grips with the subject.** And that presents a real risk for organizations! Their new digital services may never be adopted by the general public in the absence of good levels of trust. The proof: 26% of our respondents have stopped using certain services in order to protect their digital privacy and retain control of their data. It's therefore imperative that organizations respond by focusing on building, or rebuilding, relationships—based on solid footings.



MAKING ORGANIZATIONS MORE ACCOUNTABLE ON A GLOBAL SCALE

THE GDPR: AN OPPORTUNITY FOR ORGANIZATIONS TO STAY AHEAD OF DEVELOPMENTS IN THEIR COUNTRY'S REGULATORY FRAMEWORK

Digital privacy has become an international subject of discussion. In 2016, our report presented an overview of the legal frameworks for personal data protection and highlighted some of the significant developments of recent years. Since the idea of an individual's digital life began to feature in legislation, the amount of regulation has increased markedly. **The European Union (EU) has positioned itself as a trailblazer of this trend through the GDPR**, **but non-EU countries are also active in the area**. In fact, we're now witnessing a global movement to put in place a structured regulatory framework covering personal data.

The GDPR applies to all EU organizations or those whose activity is directly aimed at EU residents. This quite naturally means that its concepts and requirements have to be grasped and addressed beyond Europe's borders. And the GDPR's cross-border nature has been rapidly demonstrated: the largest penalty applied so far has been incurred by a US company. Google was fined €50m in January 2019 by the French data protection authority—following a joint complaint brought by French citizens. The French authority has collaborated with its European counterparts when applying such penalties in order to ensure that common principles are applied to the judgment.

There's also an opportunity for organizations that are not directly affected by the GDPR to anticipate the way that regulations may develop within their country. On the one hand, because the digital world has no borders, protecting privacy requires a harmonized global framework. On the other, there are strong, short-term demands in this area, both at grassroots and corporate levels (something our survey results bear out). For example, Apple's CEO Tim Cook praised the GDPR earlier this year in an op-ed for Time Magazine, where he called for the US to implement a similar regulation.

Gwendal Le Grand, Director of technology and innovation at CNIL (the French data protection authority), is already working with international authorities on digital privacy: "Other authorities are also seeking, in the wake of the GDPR, to put in place national or regional legislation.» In its annual report, the CNIL signals that it is working more closely with its Asian counterparts (APPA—the Asia Pacific Privacy Authorities) to «discuss the impact of the GDPR in the region and consider the prospects for cooperation and expertise sharing.» The objective? «Successful data diplomacy both in Europe (with our counterparts in the EDPB [the European Data Protection Board]) as well as internationally» says Gwendal Le Grand.

Today, everything indicates that **the GDPR is becoming the global reference in terms of a regulatory framework to protect personal data.**

1. http://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/

THE GDPR—A FIRST STEP TOWARD DIGITAL TRUST?

GWENDAL LE GRAND, Director of technology and innovation at CNIL (the French data protection authority)

HAS THE GDPR GENERATED THE EXPECTED LEVELS OF AWARENESS?

The GDPR came into force on May 25, 2018, and is a regulation that affects everyone: organizations, individuals, and data protection authorities. People have taken advantage of their rights and have chosen to exercise them more vis a vis organizations. The result has been a significant increase in the number of complaints. If we look at the figures, the CNIL received 11,077 complaints over the last year—an increase of 32% on the previous 12 months.

WHAT AREAS GENERATE THE MOST COMPLAINTS?

To date, the complaints that the CNIL has received remain fairly «traditional.» They mainly relate to the desire to control information that appears online (delisting; the deletion of content from blogs, news sites, or social networks; etc.). There are also large numbers of complaints about commercial prospecting and HR-related issues. In this last area, it is surveillance activities, in particular, that generates complaints: being monitored at work—the monitoring of activity or video surveillance. We're also seeing the emergence of collective complaints. In particular, these complaints are coming from associations like la Quadrature du Net and NOYB (led by Max Schrems), one of which has recently resulted in the largest penalty ever applied by the CNIL.

AND, TAKING AN INTERNATIONAL PERSPECTIVE, WHAT'S YOUR ASSESSMENT OF THE STATE OF AFFAIRS?

Our goal is successful data diplomacy with our European counterparts at EDPB level, as well as on the wider international stage. We're in discussions with a number of countries and regions that are seeking to put in place national or regional legislation in the wake of the GDPR. In particular, we've been working with Asian partners, the US, and within the framework offered by Council of Europe Convention 108. And, obviously, this work is ongoing.

In terms of investigations and penalties, what's your assessment of things, and what does the future look like?

Taking the figures, last year we carried out about 300 investigations (online, on site, or on documents) and we issued 11 penalties in France.

As we know, the power of the authorities with respect to penalties has increased significantly with the arrival of the GDPR. For a long time, the maximum penalty that the CNIL could apply was 150k. This amount increased to 3m, in 2016, with the introduction of France's Digital Republic legislation. It now stands at 20 million—or 4% of global revenue. It should be borne in mind that the penalty procedure takes time: one stage of the investigation sequence ends with the issuing of a formal notice. The penalty procedure is normally triggered if the organization does not then comply with the deadline set out in the formal notice. The procedure is built on the adversarial principle, which is designed to ensure that the organization concerned has an opportunity to defend itself. As their investigations move toward completion, authorities are gradually making use of the new ceilings the GDPR allows.

In terms of future controls, three themes will be particularly important in 2019: the rights of individuals, subcontractors, and data relating to young people.

IS THERE ANY SCOPE FOR A HAPPY MARRIAGE BETWEEN INNOVATION AND THE GDPR?

The challenge for European legislators is to reconcile innovation and people's rights by defining the framework for responsible innovation.

Our website (linc.cnil.fr) addresses questions such as new technologies and privacy protection. We regularly publish documents covering new topics: personal assistants, blockchain, interface design, data sharing, etc.

The CNIL also provides support for startups. We're already active in places like Station F (a Paris business incubator), and we run workshops on the protection of privacy. Doing this allowed us to meet over 400 people from startups in 2018. We use these settings to explain the fundamentals of the law but, above all, to answer the questions that such players have. This then enables them to develop their business activities, while working within the framework set by the GDPR. To provide ongoing support to them, we have recently set up a dedicated section on our website https://www.cnil.fr.

THE UK AND PRIVACY—WHAT DOES THE FUTURE HOLD?

NICK PRESCOT, Cybersecurity & Digital Trust Expert, Wavestone UK

HAS PRIVACY PROTECTION BECOME A PRIORITY FOR UK ORGANIZATIONS SINCE THE GDPR APPEARED?

For many UK organizations, the impact of the GDPR has been important because it hasn't been addressed merely as a new European standard on data protection. Because of the close ties between the UK and the US, the UK is seen as a global standard setter (many international organizations choose to locate their European/African/Middle Eastern headquarters in the UK). As a result, despite the prospect of Brexit, organizations have invested in complying with the GDPR; and they continue to work to ensure that its measures will be maintained over the long term.

DOES THE PROSPECT OF BREXIT INFLUENCE EFFORTS TO COMPLY WITH THE GDPR?

Brexit, which is now postponed until October 31, 2019, isn't jeopardizing the implementation of the GDPR's provisions in the UK—it has already been transposed into national law in the UK's 2018 Data Protection Act. In fact, this legislation goes even further, since certain infractions related to the processing or misuse of personal data are now classed as criminal offenses. The main concern is the UK's possible «third-party country» status after it leaves the EU, which would require the establishment of a new data-processing agreement. This would have been expensive to implement in the case of a no-deal Brexit, but such a scenario doesn't appear very likely now. From the point when the UK Parliament ratifies a withdrawal agreement, a transition period will run until December 2020, and during this time the current situation will remain unchanged. After that date, there'll be a need to put in place a new agreement on data processing.

WHAT ARE THE PROSPECTS FOR THE COMING MONTHS IN TERMS OF PRIVACY?

The confidentiality of personal data has become an increasingly important issue for 18 to 25-year-olds in the UK. Recent scandals, such as the leaking of the details of 500m Facebook accounts and the Cambridge Analytica scandal, have made this generation much more sensitive about the data they share online. The trend is a recent one, as society gradually becomes aware of the data held on it by third parties, as well as what those parties do to protect it. Moreover, the aftermath of the data leak that affected British Airways in December 2018 will be subject to particular scrutiny: it will result in a test case—especially in terms of the level of penalty that the ICO (the UK's data-protection authority) will impose. Organizations will be watching closely to see if British Airways is fined 2% of its global revenue, something most of them fear will be the case.

SIGNIFICANT CORPORATE EFFORTS TO COMPLY WITH THE GDPR

A presentation of benchmarking work carried out with 24 organizations in different sectors, six months after the GDPR entered into force.

To gain a detailed understanding of the work organizations are doing on digital privacy, Wavestone reviewed the measures in place at 24 of its clients and assessed how their GDPR compliance programs had progressed. To do this, we leveraged data from relevant support projects conducted with these players. The goal? To estimate organizations' overall level of compliance with the GDPR and highlight the main issues and trends on the horizon, based on our experience in supporting GDPR compliance programs.

TO DATE, WE OBSERVE AN OVERALL COMPLIANCE FOR THE ORGANIZATIONS OF THE PANEL, BUT THERE ARE CHALLENGES AHEAD IF THEIR APPROACH IS TO BE SUSTAINED...

The analysis results bear this out: the organizations of the panel have grasped the GDPR's requirements and made efforts to comply. One of the positive consequences of the investments these companies have made has been a better understanding of data within their organizations. While the level of compliance that has been achieved is, in general, satisfactory, there are two areas where vigilance is required:

Ensuring full compliance on the HR side

30% of respondents went as far as to say that **the extent to which companies protect their privacy could become the main criterion when choosing an employer**

Out in the field, we often find that organizations are focusing on customer, rather than employee, data. There are two reasons for this: not to jeopardize the trust already established with customers, and to prioritize «visible» compliance—in order to not attract the attention of regulatory authorities. It's interesting to note that, paradoxically, and contrary to the trends observed on the customer side, trust in employers on the use of personal data seems to have increased (albeit weakly) in recent years. This can be explained, in part, by the historical significance that organizations have attached to protecting employee data, particularly in the context of complying with labor laws or managing labor relations. As a result, data protection expectations were generally being addressed before the GDPR's arrival, and levels of maturity in this area are already high.

While the initial approach taken may seem pragmatic, especially for B2C organizations, it's important not to neglect employee data. **Increasing levels of confidence do not mean that employee expectations, with respect to their employers, are any lower.** In fact, we find similar proportions of respondents for whom data protection within their organization is important—in the same way that it is with respect to third-party organizations.

It's crucial that organizations maintain and strengthen relations with their employees. Data handled by employers can be highly sensitive, and an employee data breach can seriously damage an organization's reputation. In the future,

having established a high level of trust will also make it easier for HR departments to introduce new technologies (such as predictive career analysis, activity management, etc.) into their processes.

Ensuring the approach adopted is sustainable

The processes that organizations put in place (responding to individuals' requests to exercise their digital rights,implementing a privacy-by-design methodology, conducting a Data Protection Impact Assessment [DPIA], etc.) are still largely "manual." What's needed is **to embed, optimize, and future-proof them**—in order to ensure that the effort that has been put into compliance isn't wasted over time. Given that the compliance deadline, of May 25, 2018, has passed, efforts should now be focused on **making compliance sustainable in the long term**, as well as capitalizing further on the gains already made through compliance programs. This requires a number of challenges to be met.

> «The GDPR involves putting in place what's known as "dynamic compliance": it requires the regular reassessment of security measures in all areas that relate to the protection of personal data. We're moving from a philosophy of compliance at a single moment in time to one of continuous improvement.»
>
> *GWENDAL LE GRAND, Director of technology and innovation at CNIL (the French data protection authority)*

...RETHINKING INFORMATION SYSTEMS THROUGH THE LENS OF DATA

The entry into force of the GDPR has revealed a pain point for more traditional organizational structures: the inability to manage their information systems in a holistic fashion.

Whereas digital organizations have made data mastery—and the ability to capitalize on it—a core driver of the value they add, some of the more basic questions raised by the GDPR pose fundamental problems for other types of organizations: What data do we collect? Where is it stored? How is it processed? How many account(s) might one individual customer actually have? Can we ensure that an individual's data is properly erased? How can we give people back control of their data? The lack of overall mastery of the IS creates real difficulties for many traditional players.

Out in the field, a number of patterns are apparent:

- **IS architecture tends to be service oriented or mirror the organizational structure; as a result,** it doesn't lend itself to an overall, data-centered approach. This leads to both a lack of unity—and a loss of opportunity: that of capitalizing on data to better serve customers. As an illustration, 55% of the organizations of the panel have to manage consents on a function-by-function basis; consequently, they can't guarantee that they will be comprehensively managed on a company-wide basis.
- The digital transformation and rapidly evolving uses have pushed many players to open their information systems up to partner organizations, quickly integrate new technologies, and develop software that meets changing business needs—but **without necessarily prioritizing the overall consistency of the architecture**. As a direct consequence, they are not managing the entire data life cycle in a coherent way—something that makes implementing a holistic approach to GDPR compliance complicated.
- Putting it in concrete terms: **for most organizations, it's technically impossible to automate data deletion at the end of the retention period or when requested**—either due to technical limitations, or because of the difficulty in gaging the potential for unintended consequences. As a result, it's proving difficult to put in place effective processes to address digital-privacy-related requests, or indeed to be certain about what the result of doing so would be. In this same vein, it's also proving difficult to address the new rights created by the GDPR, in particular those covering portability and restriction.

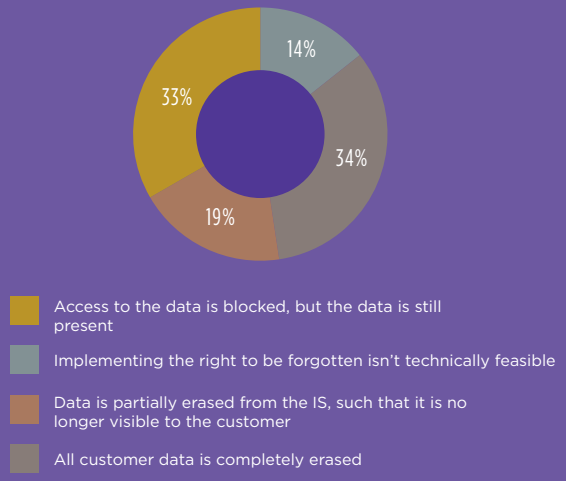
FOCUS ON THE DIFFICULTIES ENCOUNTERED IN DEALING WITH APPLICATIONS TO EXERCISE DIGITAL RIGHTS

Some organizations may find that meeting deadlines to deal with a digital-rights-related request is more complex than they had anticipated. Our benchmarking work reveals a gap between being able to handle traditional data rights and handling the new rights conferred by the GDPR. Over three quarters of the organizations of the panel consider that they master of traditional rights, including the rights of rectification and access. Conversely, the right to object—and new rights, such as the rights to erasure, restriction, and portability, are coming up against barriers of technical complexity and conflicts of interest.

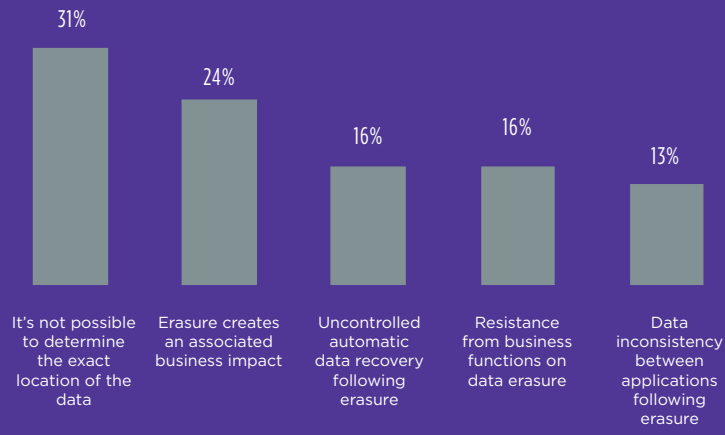
FOCUS ON THE RIGHT TO BE FORGOTTEN

Only a third of the organizations of the panel have reached a point where they can guarantee the removal of the entirety of a customer's data under the right to be forgotten. They are experiencing technical challenges as they try to implement the measures associated with this right. In addition, organizations are facing reluctance, across different parts of their businesses, to erase data—due to the absence of a comprehensive view of the potential for unintended consequences.

HOW DO YOU HANDLE THE RIGHT TO BE FORGOTTEN?



DIFFICULTIES FACED BY ORGANIZATIONS WHEN PREPARING FOR THE USE OF THE RIGHT TO BE FORGOTTEN



FOCUS ON THE RIGHT TO OBJECT

The complexity associated with this type of request is closely linked to obtaining consent. Organizations have put in place interfaces that allow requests to be made and received, but these work on an application-by-application basis; in the majority of cases, this automatically carries the risk of treating users inconsistently.

FOCUS ON THE RIGHT TO PORTABILITY AND RESTRICTION

These two rights have not been prioritized in GDPR compliance programs as a result of a lack of feedback from experience and sector-specific guidance. It should be noted, however, that these rights have been little used to date.

The ideal for organizations would be **to increase the number of omnichannel single sources of truth**. In other words, to structure their ISs around master databases that cover all users—whether the questions are related to applications or individuals. For example, where there is a single source of truth relating to a customer's postal address, a change in address can be replicated in the IS by simply reporting a change in that one database. **There are numerous advantages to this approach: data is consistent, true in all places, and it becomes much easier to handle requests to exercise digital rights.**

THE NEED TO PUT IN PLACE A SINGLE SOURCE OF TRUTH

PASCAL VIDAL,
Cybersecurity & Digital Trust Expert, Wavestone

WHY DO ORGANIZATIONS HAVE TROUBLE MASTERING CUSTOMER DATA?

To understand this, we need to go back to the origins of corporate information systems (ISs). The IS, like the organization itself, will have been designed to meet urgent needs for technical support from the business functions, with each need (web application, mobile app, loyalty program, after-sales service, logistics, store, etc.) having its own application and data repository.

As a result, businesses find themselves with an IS that mirrors their functional silos, with as many customer databases as there are applications. In other words, the IS doesn't offer a global view of customer data—or the opportunity for data mastery that such a view would bring.

WHAT ARE THE ISSUES FOR COMPANIES AND HOW CAN THEY BE HELPED TO PROPERLY MASTER THEIR CUSTOMER DATA?

In an age of data protection regulations, the main challenge for companies is **to build relations of trust with their customers.**

This trust is to be built on both transparency about how customer data is processed, and, in particular, **on making customers the masters of their personal data—by facilitating their access to it.**

This requires companies **to rethink their ISs through the lens of a comprehensive, data-driven approach which places customers at the center of considerations:** Which data belongs to the customers? Where is it? How can it be accessed? In what ways is it processed?

Nevertheless, companies are having difficulties with this new approach: they need to contend with an IS whose structure is a result of other imperatives—and therefore not very agile—as well as the need to link it to new sources of, mainly digital, data (for example, social networks).

Such difficulties are symptoms of what is essentially lacking in organizational ISs: a single source of truth (SSOT) that assures the cross-functional management of **data—the repository of customer identities.**

HOW BUILDING A REPOSITORY OF CUSTOMER IDENTITIES CAN ACCELERATE GDPR COMPLIANCE FOR ORGANIZATIONS

A customer-identity repository can act as the central hub for customer data management. Its role is to collect, centralize, and make such data available to all company systems, both physical and digital.
And, beyond this central role, it can enable organizations to more easily meet the GDPR's requirements, by:

- Knowing **what personal data the organization holds**, and in which systems, through an aggregate view of the data which we'll refer to as the «customer identity.» This identity will serve as the central point to connect the entirety of a customer's personal data and the systems that have access to it.
- **Making customer data reliable**, in order to control its quality and update it in all relevant IS systems—regardless of the point of contact (stores, digital channels, customer service, etc.).
- **Making customers masters of their own data,** by giving them access to a centralized view of the personal data held on them, which enables them to exercise their rights (rectification, erasure, the right to be forgotten, etc.).

A project aimed at building such a repository of identities may take time, especially for large organizations. However, today, turnkey solutions are available that can be used to rapidly create a repository: **Customer IAM solutions** (Customer Identity and Access Management).

WHAT IS A CUSTOMER IAM SOLUTION?

A Customer IAM solution aims to simplify, and make reliable, the processes used to manage and protect customer data—both for existing customers and prospects.

These solutions use technological accelerators **to create a management and data security layer that cuts across historical IS silos.**

They revolve around three main features:

- **Centralizing and sharing personal data and customer consents by providing a central identity repository that synchronizes customer data in the IS's systems**, including through the use of real-time interfaces to address the requirements created by digital channels.
- **Securing access to customer data by providing access control services for customers themselves** (passwords, social logins, single or multi-factor sign in, biometrics, etc.) and the systems processing the data.
- **Monitoring whether customer-data processing and usage is compliant** by providing the DPO and business functions with dashboards to monitor consents, personal data held, or customer preferences.

All of these solutions are part of an (API-oriented), agile and interoperable approach, which can be integrated transparently into the corporate IS.

IS A CUSTOMER IAM SOLUTION A MIRACLE CURE FOR GDPR AILMENTS?

In a word: "No". Although these solutions can provide accelerators that place a data-management and protection layer across the IS, they don't remove **the need to define and implement a global approach to customer data governance** (in terms of processes, security, processing, storage, etc.).

...PUTTING IN PLACE CONSISTENT, CROSS-FUNCTIONAL DATA GOVERNANCE ONBOARDING DIGITAL PRIVACY

Implementing a data governance approach is, then, a strategic priority for organizations. However, faced with the urgent task of complying with European regulations, organizations have not necessarily had the time to address this requirement head-on—they've generally been too busy with the immediate demands of personal data protection. To ensure that compliance is both optimal and sustainable, these two dimensions now need to be linked so that privacy can be properly embedded into practices.

It's therefore a question of rethinking strategies to capitalize on data, while also keeping in mind the regulatory requirements. The large volumes of data collected as a result of the development of digital and new technologies offer new possibilities for business functions—but also carry risks. According to a study—« la révolution de la data » [«The Data Revolution"]—conducted for Wavestone by the Infopro group, and published in May 2019, one of the main obstacles to capitalizing on data within organizations is its poor quality, something that can render it unusable. **A balance must be struck between collecting masses of data and optimizing its quality and exploitation.** In other words, it's essential to take both a quantitative and qualitative approach.

> «The principles and requirements of the GDPR require organizations to put in place a data-specific approach to governance that makes privacy issues integral to their activities.»
>
> *GWENDAL LE GRAND, Director of technology and innovation at CNIL (the French data protection authority)*

The GDPR brings this balance into focus through **the principle of minimization**—something that's not necessarily at odds with digital marketing performance. However, even though we're seeing effort being put in at ground level in some organizations, to properly qualify their databases, there are no signs of a fundamental shift in approach occurring. This is borne out by the fact that only a small proportion of organizations have launched consent renewal campaigns and the observation that only half of the organizations have processes in place to verify that the data collected is limited, appropriate, and relevant, in relation to its use.

An opportunity to be seized to desensitize data: pseudonymization!

There is a clear distinction between pseudonymization and anonymization. Anonymization is considered irreversible and therefore removes data from the scope of the GDPR (because it's no longer information «of a personal nature»). Anonymization is complicated for organizations and does not always allow the data's value to be maximized. For example, given that it removes the link with the individual, it no longer allows behavior to be followed dynamically over time. In this sense, pseudonymization is a good alternative, and is something already being exploited by some organizations.

To date, the main techniques used in pseudonymization are the use of cryptographic systems, hashing functions, or tokenization approaches. By using these techniques, a new identifier can be automatically assigned to the data collected. The identification key, which enables a link between the new identifier and relevant individual to be directly established, is stored in a database subject to enhanced security and to which access is limited to technical administrators. The pseudonymized data is stored in another database that **allows different parts of the business to analyze trends and track behavior over time.**

In contexts where it makes sense, directly pseudonymizing all data, or all data that can easily be identified (first names, surnames, email addresses, phone numbers, etc.) offers three key benefits:

- **Increased security.** Both databases (the pseudonymized database and the one that links it to real individuals) would have to be attacked to connect the data and therefore be able to directly identify the persons concerned.
- **Optimization of the data's value.** As discussed above, pseudonymized data allows the link with individuals to be kept and, therefore, their behavior to be followed over time.
- **Simpler ways to handle the exercise of digital rights within the scope of pseudonymization.** If a person exercises their right to be forgotten, deleting the linking identification key in the correspondence table would mean that using pseudonymized data comes close to erasing the personal character of the dataset. This, however, means that the data stored (and not pseudonymized) must be sufficiently well configured to avoid the individual being easily identified through a process of deduction using other information that can be viewed.

MAKING DATA PROTECTION A DAILY HABIT

96% of the organizations of the panel included **a personal-data risk evaluation step in their project methodologies but a third of the organizations of the panel don't think this is sufficient in ensuring compliance over time**

Moving from a project to day-to-day operations will always involve its share of complexity. When the enthusiasm (whether voluntary or forced) to achieve compliance is over, there's a need to maintain a data-privacy philosophy over time. And this must be anticipated!

1/4 of the organizations of the panel consider that **they have a «privacy» team designed to meet the requirements**

Our benchmarking exercise highlights, unsurprisingly, that the greatest fear of those involved in privacy work within organizations of the panel is a shortage of resources once the project phase is completed. Only a quarter of organizations consider they have a privacy team capable of the task, and the known skills shortage in the market doesn't do much to reassure them. This means that simply being prepared to invest heavily in this area won't enable teams to be strengthened overnight.

Therefore, making a privacy-centered approach work, by design and by default, despite the potential lack of resources, is a stake—even the stake—for most organizations. It seems that privacy teams won't be able to assure organizational compliance with the GDPR in the long term. How to reach the promised land? **Make the protection of personal data everybody's business**—and position the privacy team as a facilitator and coach to the business functions:

/ **Create a privacy-centered culture by educating and training employees.** If they use data on a daily basis (for example, banking data), individuals lose consciousness of data's sensitivity and, as a result, they may put the data at risk. It's therefore essential to anchor good data-protection practices firmly in daily work activities, and to make employees aware of the issues that personal data entails. In particular, making clear to marketing teams the value of high-quality consent data, and helping them to understand the benefits of an appropriate strategy, will help reduce the number of inappropriate communications and therefore complaints.

/ **As time goes by, this lens of awareness.** To date, internal communications about the GDPR have revolved around fear (inspections, fines, etc.). But, to embed best practices, it won't be sufficient to repeatedly highlight the potential impacts of non-compliance. Employees need to be engaged in a more positive approach **to building trust** with the individuals who allow the organization to hold their data. There will also be a need to give them the tools and concrete operating procedures that will underpin this trust building.

/ **Getting the business functions to take ownership.** The data-protection dimension must be an integral part of their professional activity, like any other, and not seen as a burden. In a purchasing department, for example, keeping an up-to-date list of partners to whom data is transferred, or including GDPR clauses in an agreement, should happen as naturally as negotiating a contract. We're seeing strong positive momentum in this area, with 91% of the organizations of the panel having carried out the work of identifying the relevant partners, transfers, etc. In order not to waste the investment made, there's a need to maintain this effort over time by capitalizing on the work done on contracts and ensuring that the GDPR is considered naturally in the normal flow of work. One way of achieving this may be to explicitly include privacy goals in employees' job descriptions and/or development plans.

/ **Implement a form of «agile data protection» that's easy to use.** It's essential not to place additional stress on the processes already in place, otherwise privacy issues will be systematically perceived as a burden. Privacy by design must be organized simply, to be accessible and understandable for project managers, in order that they can be as autonomous as possible on the subject.

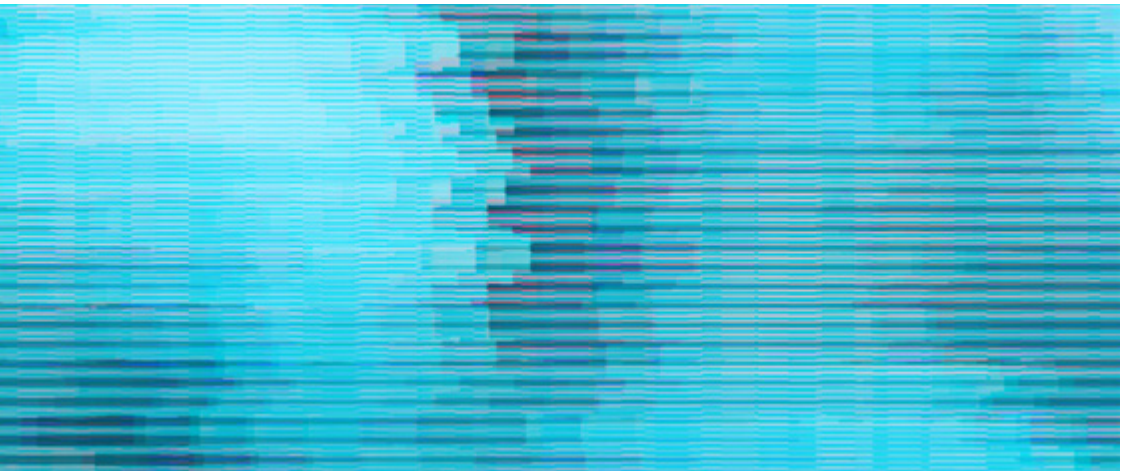
/ **Positioning the data privacy team as an innovation facilitator.** According to a study—« *la révolution de la data* » [«The Data Revolution"]—conducted for Wavestone by the Infopro group, and published in May 2019, only 37% of organizations of the panel considered GDPR compliance an asset. This represents a risk to sustainable compliance. In addition, those working on privacy shouldn't be consigned to a role of running projects that ensure good regulatory compliance; they should also have an advisory role and contribute to innovation. In order not to put constraints on business functions, and to strike the right balance, it's essential to understand the issues and challenges they face—and, as a result, be able to play a part in the deployment of new technologies within the organization. Effective monitoring is key to this—to be able to anticipate and identify new risks relating to data generated by innovative solutions. Typically, in the world of large-scale retail, DPOs will need to improve their digital marketing skills, and their understanding of offerings like Google Ads or Critéo. Doing this will enable them to respond more quickly to the questions business functions might ask, and make recommendations to them in advance, etc. With this in mind, and to support organizations, the French

regulator has set up an innovation center, LINC, which anticipates questions and considers how to fuse innovation and compliance. In particular, the center has worked on issues like interface design, voice assistants, etc.

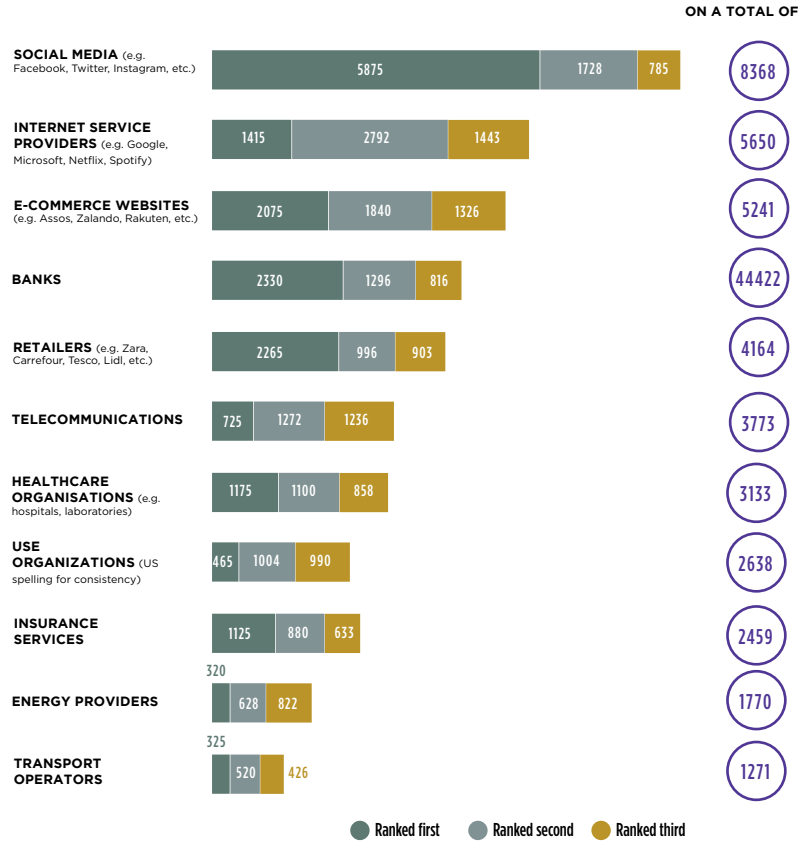
Rethinking processes to maintain a good level of compliance will still require effort from organizations. But compliance is not an end in itself. The public survey shows that their understanding of the GDPR is far from perfect (for at least three quarters of respondents). As an example, we see that banks, the sector that invests most in its compliance, and which is most familiar with the types of compliance programs required, have lost their most recent position of third place—in terms of being the players in whom customers have the most confidence.

Historically, **banks** have been among **the players most trusted by customers**. In 2016, 51% of respondents put banks in first place in terms of trusted third parties...

...today, **banks have fallen to eighth place** in the rankings of trusted players for data protection. 10% of respondents even cite banks as the type of organization in which they have **the least trust.**



WHAT TYPES OF ORGANIZATION DO YOU LEAST TRUST TO USE YOUR DATA ONLY FOR THE PURPOSE YOU'VE AGREED TO?



These findings demonstrate clearly that, while compliance with regulations might be a necessary condition—it's not a sufficient one—when it comes to gaining or maintaining people's trust. It's also about persuading the stakeholders involved. Brands will have to innovate to adapt to changing consumer orientations and purchasing behavior. **The safeguarding of privacy has the potential to create value for organizations that know how to make it a selling point, or even monetize it, as well as the potential to generate new models and new organizations.**

SHOULD YOU GO BEYOND THE GDPR WHEN IT COMES TO PRIVACY?

SOME REAL BUSINESS OPPORTUNITIES EXIST

In fact, the GDPR, and privacy more generally, offer real opportunities for organizations. These all involve innovation: from new constraints to new solutions. The first initiatives are already emerging and have become talking points, as evidenced by an infatuation with privacy issues at CES 2019.

> «Innovation, breakthrough ideas, and great features can go hand in hand with user privacy—and they must. Realizing technology's potential depends on it.»
>
> *TIM COOK, CEO Apple, Magazine Time*

There is a great deal of thinking around new solutions and new business models; these are more bullish and differentiate themselves on privacy protection and providing people with control over their personal data. We discuss some examples below.

MAKING PRIVACY A DIFFERENTIATOR

Responding to the challenge of digital trust should not be seen solely as a regulatory or security issue; rather it should be viewed as a fundamental transformation in customer relations and digital uses. **Turning privacy into a generator of revenue**: the ultimate objective. Today, we're still in a phase where a culture of privacy is developing and spreading: people are becoming progressively more aware of issues related to their private lives. As a result, they are increasingly inclined to opt for services that safeguard privacy. But this movement could be about to be strengthened.

Confidence is becoming a strong indicator of effective differentiation in customer relations. There are a number of options to consider here. The challenge? To be able to demonstrate ever-increasing transparency and build a deep relationship of trust between an organization and its customers.

Strengthening customer relations by giving people control over their data

In order to help customers take responsibility for managing their own data, and to be more transparent, some organizations, such as Adidas and Asos, have already set up privacy centers. A privacy center is a personal space where users can view and manage their personal information, adjust their preferences and consents, and easily make use of their rights. By making users masters of their own data, privacy centers provide a measure of trust and transparency on the part of the organization and ensure a better customer experience. Such platforms, because they are automated and the only point of interaction on data privacy, greatly facilitate the scaling up of activities, especially when it comes to all things related to the exercise of consumer rights.

However, to date, privacy centers have proved complex to integrate into information systems. Doing so requires a perfect interconnection between the interfaces (mobile, website, physical, etc.) and the various existing customer databases (because the view of the customer is rarely completely unified). Therefore, recasting the IS and putting in place true data governance will be, for most so-called traditional organizations, a question of size. **Conversely, purely digital organizations, that have built their ISs around data and the customer journey, can envisage implementing such an approach in the short term.**

However, despite being able to improve customer trust over the long term, putting in place a privacy center can initially be perceived as a risk by marketing and digital teams. The provision of a tool that can facilitate the exercise of rights, and in particular the withdrawal of consent, may give rise to concerns. There has to be evidence that real change needs to be implemented, and privacy governance must have reached "cruising speed,» before you consider putting in place such a solution.

Differentiating yourself from competitors through a privacy-oriented marketing strategy

As discussed previously in this article, there is a substantial gap between organizations' efforts on compliance and people's perception of these efforts. Therefore, organizations face a real challenge: **that of moving from a compliance project mindset to one of communicating and demonstrating the value of their compliance efforts to the general public**. Is there a champion in this respect? There is: Apple. At CES 2019 in Las Vegas, Apple demonstrated a bullish communication strategy aimed at distinguishing itself from its competitor Google. While Google had peppered the city with advertising posters to promote its new voice assistance technology, Apple contented itself with an imposing poster highlighting its slogan, «What happens on your iPhone, stays on your iPhone"—with a link to Apple's privacy platform. Apple has decided clearly to use its strong stance on privacy to differentiate itself from its competitors. Is Apple in the vanguard of a trend that's about to become more widespread? It wouldn't be the first time.

The French regulator is putting in place **a certification system that will help encourage this trend.** Two frameworks for DPO certification have already been adopted by the CNIL. In the long term, we might even see the establishment of a label that certifies good organizational compliance with the GDPR. Thinking on this is already underway in regulatory circles.

Such marketing strategies help raise awareness of the importance of privacy and how it applies in the digital world. **And today, for those who seize the initiative on privacy, they offer a route to competitive advantage. In the long term, neglecting privacy issues could become a real handicap for some companies.**

TURNING PRIVACY INTO A NEW SOURCE OF REVENUE

1/3 of respondents would **be willing to pay for higher levels of privacy protection, and for services that better safeguard their data**

In our 2016 study, Tina A. Larsen (the head of Luxembourg's regulatory authority) told us, «people want to benefit from the services that mass data collection can generate (more personalized services, social networks, etc.) while also protecting their privacy.» What's the right balance to strike? It seems, in any case, that people need to be given a choice.

After analyzing our results, we considered what might be the appropriate offering for the "privacy absolutists"—the 25% of respondents who are unwilling to share their data. We asked respondents whether they already used, or would be inclined to pay for, a service that better protected their privacy.

It seems that a shift is already well underway beyond Europe's borders. In China and the US, 18% of people say they've already paid an additional fee for a service that better protects privacy, compared with only 5% in Europe (including the UK). Europe is behind in offering privacy-protection services.

It has a real corner to turn. Especially given that the demand is there: A third of those surveyed would be willing to pay for increased levels of data protection and services that better protect their privacy. Privacy-as-a-Service—a seam to be mined?

In analyzing the areas where people would be most inclined to pay for a service that protects their personal data, it appears that social networks, internet-based services, and banks, would be the sectors with greatest demand. In these sectors, at least, there are real opportunities to design innovative, and potentially paid-for, services where the collection and use of personal data would be minimized—with the aim of meeting the expectations of this new consumer category. As already discussed, if organizations do not develop these new types of services, the percentage of respondents that fall back on anonymity or stop using certain services may continue to grow in the future. Are we moving toward a paid Facebook model?

Clearly some users will still want free services and will be prepared to accept the associated advertisements. Others will be willing to pay for services that offer greater protection.

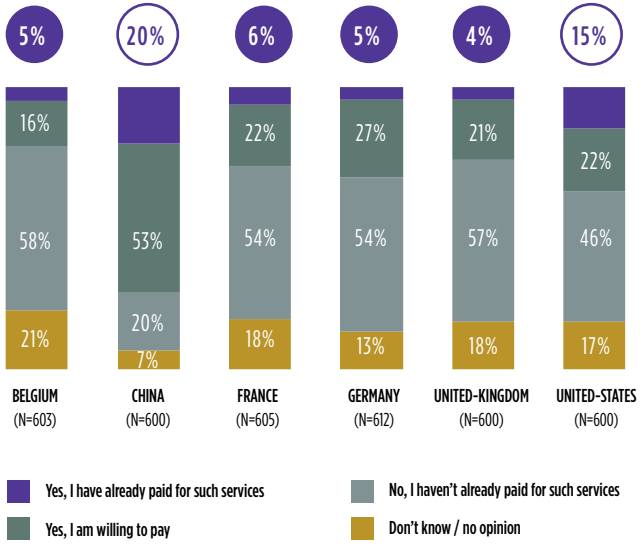
MAKING PRIVACY THE BASIS OF A NEW OFFERING

Legislation alone is not sufficient to enable individuals to control their data and protect privacy. We must give them tools that enable them to take the concrete actions that will protect their data. We're already observing that new organizations have been created around the protection and management of personal data. Wavestone has taken an interest in two emerging trends with the potential to restore confidence: self-data and 0 data collection.

Pursuing a self-data approach

The challenge here is to respond to the «crisis of confidence» arising from the asymmetry of information between

Would you be willing to pay a small fee or a small price increase for products/services, that would otherwise be free, in exchange of the guarantee of your privacy?



organizations and their customers—**by putting data back in the hands of the latter**. With self-data, organizations have access to information but no longer own it. Individuals remain the sole owners of their data. This allows them to create value through new uses for the data, something done on their own initiative and under their control.

As a result of an initiative launched in 2011 by the White House, the idea of the «Green Button" came about in the US energy sector. This lets citizens download energy consumption data from various sources in a standard format, enabling them to connect it and optimize their consumption, but also offering them the option to transfer it automatically to third parties they have authorized to receive it. This type of approach has also been put in place to handle health data, especially sensitive data, through the concept of the «shared medical file». This allows individuals to closely manage who can access their data—for example, to allow medical staff, other than an attending physician, to access certain data temporarily.

Are we moving toward the wide-scale adoption of this approach?

COZY CLOUD INTERVIEW

BENJAMIN ANDRÉ, co-founder and CEO of Cozy Cloud

TO WHAT EXTENT DO YOU FEEL THAT PEOPLE ARE CONCERNED ABOUT PRIVACY ISSUES?

They're still not really of great concern except for a minority of people (polls suggest about 5 to 10% of the population). People in this minority understand clearly that they are pawns in a commercial game, and, as a result, there is a high degree of interest in their behavior. But, an interesting observation is that there is, today, it's no longer just «geeks» who are aware of this, it's a much greater diversity of people. This translates into the annoyance, sometimes even exasperation, that comes from the feeling of being a commodity. People are beginning to find the power of the internet giants disturbing: big tech players are becoming the bad guys.

HOW HAS THIS TREND MANIFESTED ITSELF SINCE THE GDPR CAME INTO FORCE?

I feel that the issues are now better understood, especially when I give my standard pitch; and I think the reactions I get provide a good sense of where things are at present. Four years ago, I was considered a madman in some quarters: "Confidentiality doesn't interest anyone»; «the GAFA [Google, Apple, Facebook, Amazon] model is the only one that works for the internet»; etc. Today, this is no longer the case: it's a huge milestone—and demonstrates very tangible progress.

WHAT DOES COZY CLOUD PROVIDE THAT CAN HELP?

Today, our digital data is dispersed widely. Our digital life is fragmented because its scope is so diverse: school life, health care, interactions with public authorities, connected objects, and so on. The data in these areas flows around in distinct and closed ecosystems; and that creates friction. As a result, the utility we gain from them is dampened and constrained. For digital to be useful, practical, convenient, and personalized, you have to unify the data. Doing this removes the friction between these closed ecosystems and simplifies digital uses—something that offers enormous value. Cozy's whole idea is **to centralize individuals' data in personal clouds; these are controlled by the individuals, allowing them to access new digital services**. And lastly... taking back ownership of your data is the best way to pool it.

WHAT SERVICES DO YOU OFFER TO INTERNET USERS?

Cozy cloud is not just a «static» safe, which we tend to see a lot. Users centralize their data in a personal cloud **that lets them nest services, add uses, and link various sets of data**. We might call the result «cross-cutting data»: communicating with your numerous suppliers through a single platform, and accessing new, purely digital services—**and doing all this while storing your data locally in your own digital safe**. So, **we enable individuals to access services without giving up control of their data.**

AND WHAT DOES THIS MEAN FOR ORGANIZATIONS?

That data can have a value beyond simply monetization. **The value comes not from the data as such, but rather from getting it to interact in a way that's valuable.** Organizations need to understand this. We position ourselves as a digital-interactions operator. Adopting this approach will enable them not to be permanently cut out of the loop but, on the contrary, to have access to even more data.

THIS DOESN'T NECESSARILY SEEM LIKE SOMETHING OBVIOUS AT FIRST SIGHT: HOW CAN YOU PERSUADE THEM?

Today, the feedback is unequivocal: the GAFA companies know more about bricks-and-mortar companies' customers than bricks-and-mortar companies do themselves. On the other hand, bricks-and-mortar companies have the advantage of high levels of historical trust. **Our customers are large players, to whom the internet majors are a competitive threat; they want to reposition themselves for the digital age and derive value from the asset that is trust.** Initially, organizations may have the false impression that their data is being appropriated. But in reality, what Cozy Cloud is doing is helping them develop smarter tools and uses. Either these organizations open the door to this themselves, which will prove to be a good thing for them, or Google will do it instead...

Organizations that are especially mature in privacy terms are already in a position to launch services in this area to differentiate themselves. We might even imagine, much further into the future, individuals being able to charge for access to their data. Could personal data become the new currency? In Europe, this idea is decried: the state protects its citizens, perhaps even against their will, but it's for the common good (such as in the case of the sale of organs). But, ideas like this are being envisaged elsewhere.

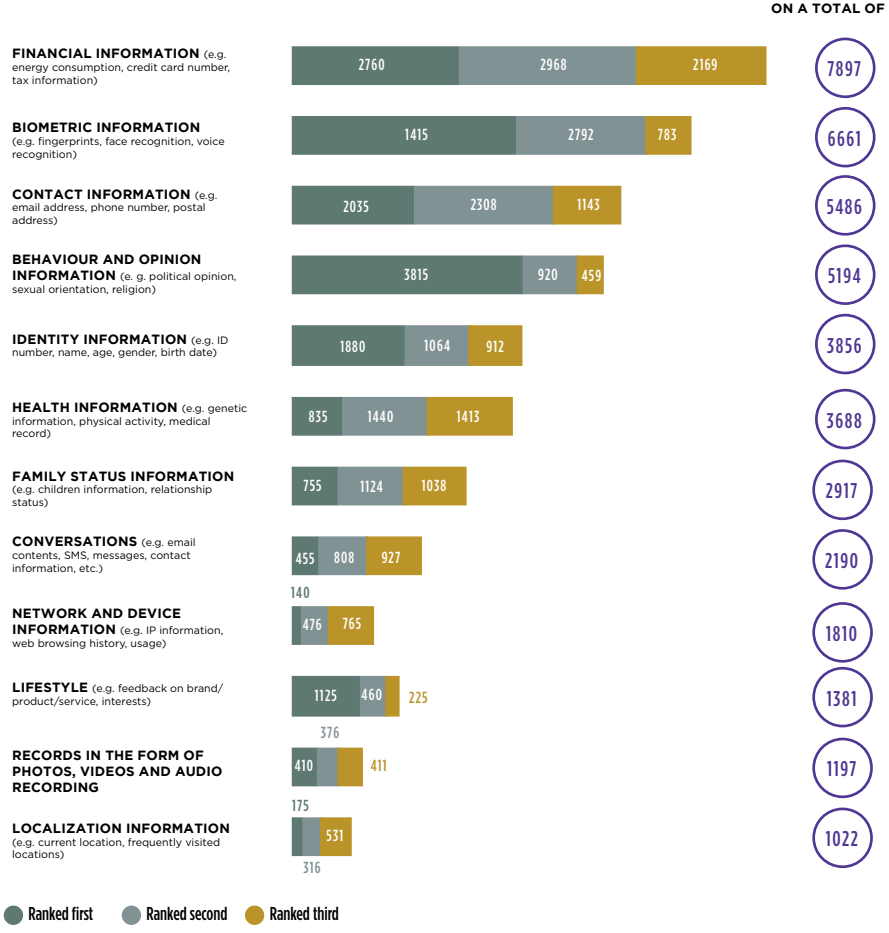
Service offerings that don't involve any data collection

Throughout our survey, we observed a deep mistrust toward internet players, especially social networks. Why?

/ **People seem to be caring more and more about their online reputations.** In its annual report, the French regulator highlighted the increasing number of complaints about data being disseminated via the internet (which amount to 37.5% of all complaints). There are real opportunities for companies prepared to go against the business models deployed by the internet giants—to bring forward a completely different offering.

/ **Another observation from the survey is the trend toward anonymity.** Because of their «gateway» status in terms of privacy, whether physical or digital, contact and identity data are the types of information most cited when people are asked about data they consider to be private. In fact, they're more frequently cited than the types

Which of the following types of information would you consider the most private?



Moreover, we're already observing people adopting new uses to preserve their anonymity and protect privacy. This is a sign of the potential future importance of anonymity.

THE POTENTIAL FUTURE IMPORTANCE OF ANONYMITY

47%

of respondents reject **COOKIES** when visiting a website.

44%

of respondents manage **PRIVACY SETTINGS** (including withdrawing consent)

27%

of respondents use **INCOGNITO MODE**

18%

of respondents use **CYBERSECURITY TOOLS** to protect their data (VPNs, etc.)

26%

of the respondents **HAS STOPPED USING CERTAIN SERVICES IN ORDER TO PROTECT, AND RETAIN CONTROL OF, THEIR PERSONAL DATA.**

QWANT INTERVIEW

TRISTAN NITOT,
VP Advocacy, Qwant

WHAT IS QWANT?

Qwant is a French company whose main product is a search engine with two specific features. The first is respect for its users' privacy: **it doesn't leave cookies or collect any personal data.** The second is that it is sovereign—and European. It covers all European languages and meets the strategic need for a European search engine because each main country has its own version of the engine. In short, Qwant has positioned itself as a responsible digital player, with a considered and ethical business model.

HOW HAS QWANT'S OFFERING BEEN RECEIVED BY USERS?

Qwant's offering has been very well received: the sense of relief among users is quite marked at times. Having said that, awareness levels on digital privacy are still far too low, in my opinion. Of course, we're seeing a trend toward increasing awareness: the GDPR is a talking point and recent scandals have had real educational value (for example, we noticed spikes in the use of Qwant following media coverage of the Cambridge Analytica and Snowden stories). However, there's still a long way to go, and a real step change in levels of digital hygiene needs to be adopted. I still feel obliged to explain to my audience, as I do almost systematically, the business model used by the internet giants. **What individuals don't realize is that they are users—not customers—of a service where the true customer is the advertiser.**

WHAT DOES THE FUTURE OF SEARCH ENGINES LOOK LIKE?

Today the digital economy is on a trajectory toward consolidation. A handful of internet giants, like Google and Facebook, collect the maximum amount of personal data by default; by doing this, they build a deep understanding of their users, which allows them to personalize and improve their services. **Such data collection goes against all ideas of minimization**. And it's not a viable solution either, because it works against individual liberties, and it's toxic for society. That's why there's a need, I think, to bring forward alternatives that ensure respect for privacy.

HOW ARE YOU PLACED, GIVEN THIS NEED?

If we want to see a sustainable approach to digital, we have to rebuild trust with users and respect their rights on privacy. The way to do this is by decentralizing and minimizing data collection by default. Qwant has positioned itself as a new-generation service provider that respects its users' privacy; it's an approach that's ethical and, we hope, sustainable.

A BUSINESS MODEL THAT RESPECTS PRIVACY... DOES THAT HAVE TO BE A MODEL WHERE NO PERSONAL DATA IS COLLECTED?

Not necessarily. However, we have to leave people with the choice—so that they're in control. Qwant is developing a new product called Masq, which saves people's searches locally on a computer or smartphone. Only users will have complete control over their search history, which can be used to refine the search engine's suggestions.

CONCLUSION

The data revolution will never take place without trust...

The development of digital is fueling fears for users, something compounded with the emergence of consumer associations that are positioning themselves as internet privacy champions. Regulatory authorities are tightening their frameworks to protect people from increasingly data-hungry organizations. Their objective? To enable people to preserve their digital privacy.

For organizations, **it's high time to approach digital differently**. Most organizations have already understood the new reality: the data revolution can't take place without trust. We observe a dynamic developing within organizations in this area, as well as efforts to minimize data collection, qualify databases (by seeking fresh consent where necessary), be transparent about how data is processed, and empower people with respect to their data—by offering them opportunities to exercise their digital rights. A trust relationship is a fragile bond, and it will be essential to respect long-term commitments if this trust is to be sustained into the future.

We're moving from a data era—built on the mass collection of data, and successful business models based on its resale—toward an era of trust. And this transition can be seen clearly in the results of our survey: in the future, people will be less and less inclined to share their data with third parties that they don't consider trustworthy. Today, more traditional players can capitalize on the historical trust they have built up with the general public; whereas digital players have a greater mastery of data and, as a result, better knowledge of their customers. We anticipate that these two worlds will converge in the near future.

...It's now a matter of thinking of new ways to place trust at the heart of customer relations—and ways to move beyond mere compliance.

The GDPR is, by nature, a regulation that encourages different disciplines within organizations to collaborate—often disciplines that have never worked together before! **It's imperative that organizations capitalize on this positive momentum.** What should their objective be? **To rethink data uses and imagine what future customer relations will look like**: **more symmetrical, and generators of trust and business growth**. Organizations need to invest now—before it's too late!

The Positive Way

WAVESTONE

www.wavestone.com