THE GDPR AND DATA PROTECTION IN EUROPE: ONE YEAR LATER

A DOSSIERPLUS ON THE GENERAL DATA PROTECTION REGULATION AND ITS CONSEQUENCES IN EUROPE

statista

Table of contents

01 The GDPR explained

- GDPR essentials
- Complaints & data breaches
- Costs of data breaches

02 Challenges for enterprises

- Challenges of GDPR compliance
- Compliance impact
- Privacy professionals

03 Data-driven marketing

- Privacy policies on websites
- Online traffic and ad vendors
- Third-party tracking

04 Current and future trends

- Data masking & data platforms
- The next ePrivacy Regulation

05 Privacy awareness

- Trust in data processing
- User awareness of personal data

06 Key takeaways

Glossary

Sources

01 The GDPR explained

- GDPR essentials
- Complaints & data breaches
- Costs of data breaches

> *GDPR is forcing a level of maturity for organizations*
> *by requiring them to know*
> *where their personal identifiable information is*
> *and where it’s going.*
>
> *(Harvey Jang, Global Data Protection and Privacy Counsel*
> *at Cisco Systems)*

GDPR: one year later

The aftermath of the General Data Protection Regulation

The General Data Protection Regulation (GDPR) was enforced in May 25, 2018 and it has been a major test for data governance in companies operating in Europe. One year after GDPR introduction, this DossierPlus gives an overview of the impact of the regulation and illustrates next challenges and opportunities related to data protection in the EU.
Further insights illustrate the effect of the GDPR on online traffic and marketing. As the regulation requires the users' specific and informed consent every time data is processed for a specific purpose, advertising vendors who use technologies to track users online saw an immediate decrease in their online reach. Mostly, the GDPR limits the use of data for advertising purposes through third-party tracking, and it enhances the importance of direct marketing for first-party data - information more easily collected by companies among their own audience.

This DossierPlus paints a picture of a post-GDPR-enforcement world, with possible trends under the next ePrivacy Regulation, which will define an even stricter use of tracking technologies by 2020. Most importantly, by setting higher data protection standards, both regulations on data protection encourage a wave of awareness among companies and individuals regarding the responsible use of data. Personal information about customers is the commodity companies will compete for. Once data is obtained, introduced obligations require any data company or organization to protect users' data efficiently. Privacy protection enforced by the GDPR will enhance investments in transparent and safe data storage. This might result in greater use of data masking technologies and more structured management of customer data, as the figures concerning these market segments suggest. A more responsible data governance will be part of corporate agendas, and future data protection will be achieved, to quote the regulation, *by design and by default*. This means that any innovation procedure will require transparency and a data privacy risk-based approach.

GDPR essentials

What is the General Data Protection Regulation ?

WHAT IS GDPR ?

The General Data Protection Regulation (GDPR) went into effect on May 25, 2018, and set the rules for **personal data processing** across the European Union. Even companies or organizations (so-called data controllers) not based in the EU must meet GDPR requirements if they process data of European citizens.
GDPR was necessary for two reasons: firstly, the latest European Data Protection Directive dated back to 1995, and offered an insufficient legal framework regarding digital media use. Secondly, it replaced the existing standards of national legislations, assuring equal data protection across all 27 EU countries.

INDIVIDUAL RIGHTS

Under clear consent of individuals, the GDPR guarantees a lawful and transparent data processing and protects the following individual rights:

Right of access and rectification of given data

Users have the right to access any information a company or organization keeps about them. Also, they can ask for that information, if not accurate, to be rectified;

Right to erasure

Users have the right to be “forgotten”, i.e. they can get their data erased;

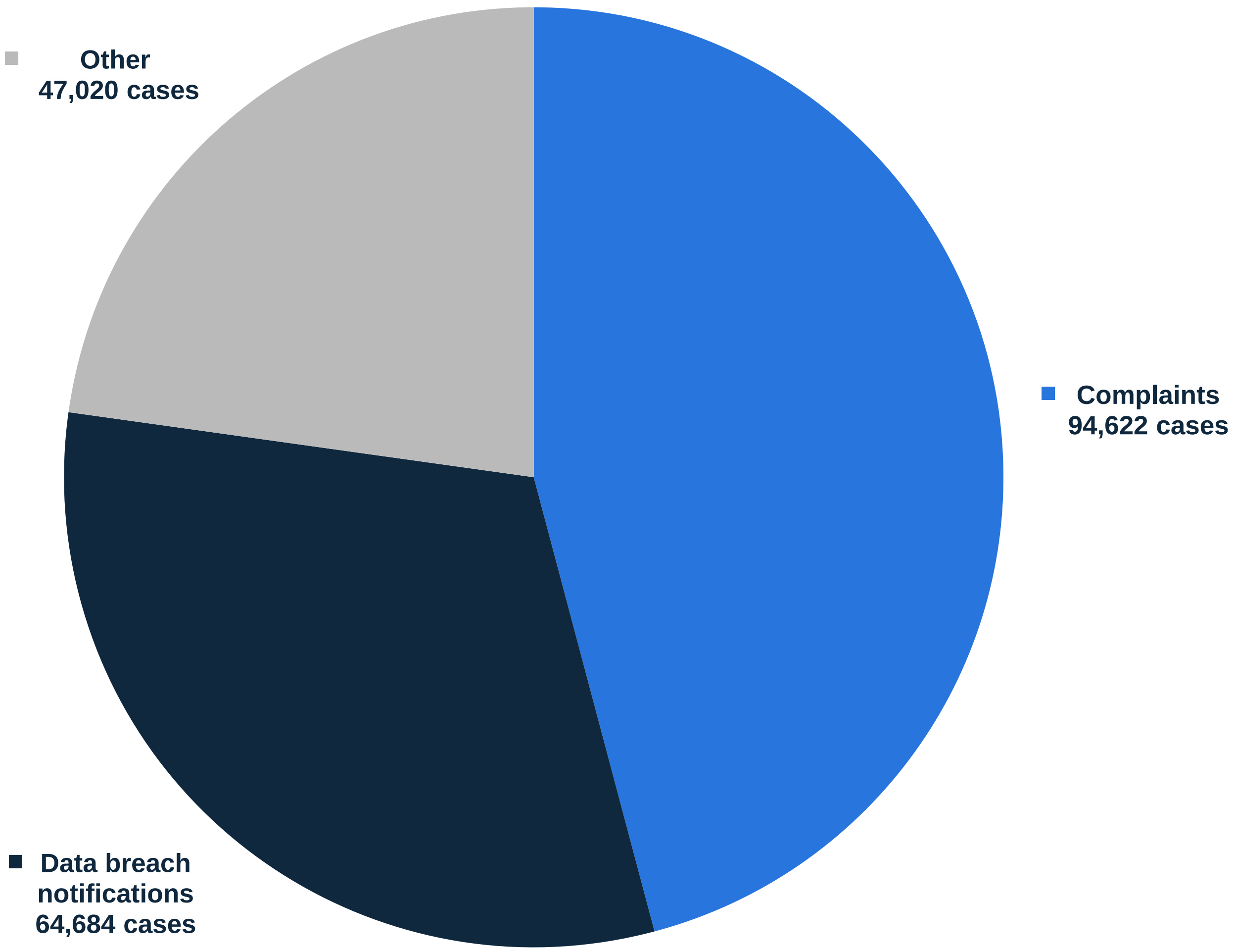
Right to data portability

Users can decide to transfer the already given data to a third party. Such request entails that companies must keep clear records of users’ personal information in a secure format. For instance, any service provider must give detailed information on the tracked user’s online behavior, as the user might decide to forward such data to another competing provider.

OBLIGATIONS

The regulation defends the rights of individuals against inappropriate use of data by data controllers and processors. To specify, data controllers must undergo specific obligations, like the release of a Data Protection Assessment, a protocol assessing potential risks of data processing. Companies and organizations are legally responsible for **data breaches**, i.e. the release of confidential information without consent. Data breaches must be detected and communicated to the users within 72 hours. Furthermore, companies and organizations handling large datasets in their core activities must appoint a Data Protection Officer (DPO), a professional figure ensuring effective compliance to the GDPR.
Cases of non-compliance to the GDPR can be sanctioned with fines up to 20 million euros or 4 percent of the global annual turnover of the data controller.

Cases of non-compliance to the GDPR up to February 2019



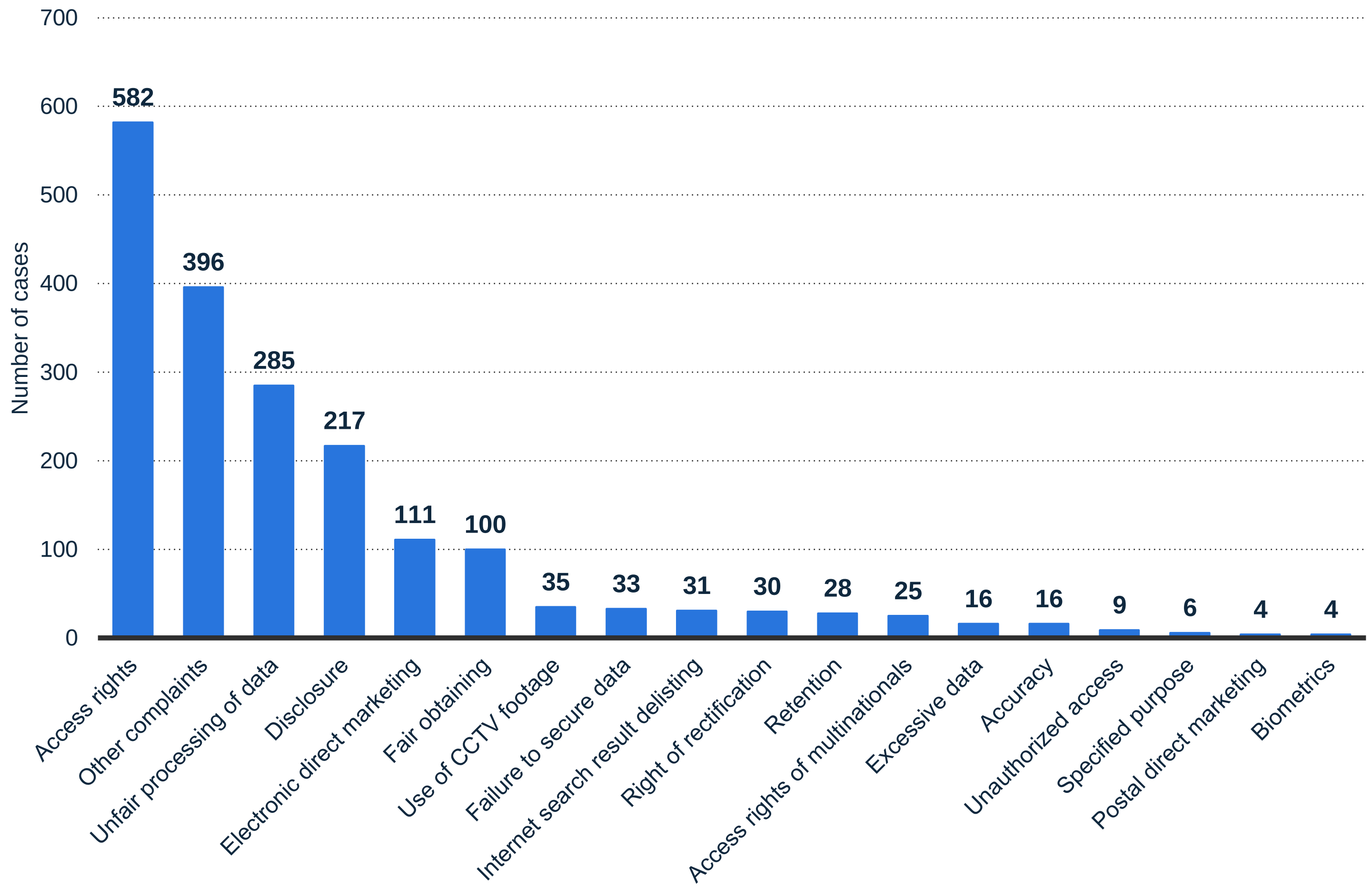
In the EU countries, cases of non-compliance with GDPR requirements are reported to national supervisory authorities responsible for the GDPR's application. 206,326 cases of non-compliance have been reported since the regulation enforcement in May 2018. That means an average of over 764 cases a day. Almost half of the reported cases are complaints made by individuals, while over 64 thousand cases were data breaches reported by companies or organizations. Under the GDPR's obligations, the reporting of data breaches by data controllers is mandatory.

Data released by the European Parliament indicate that 52 percent of non-compliance cases have been closed already, while 47 percent are still ongoing. The remaining one percent is made up of appealed cases.

Note: EU; May 2018 to February 2019
Source(s): European Parliament; Various sources (Privacy Supervisory Authorities of 31 EEA countries)

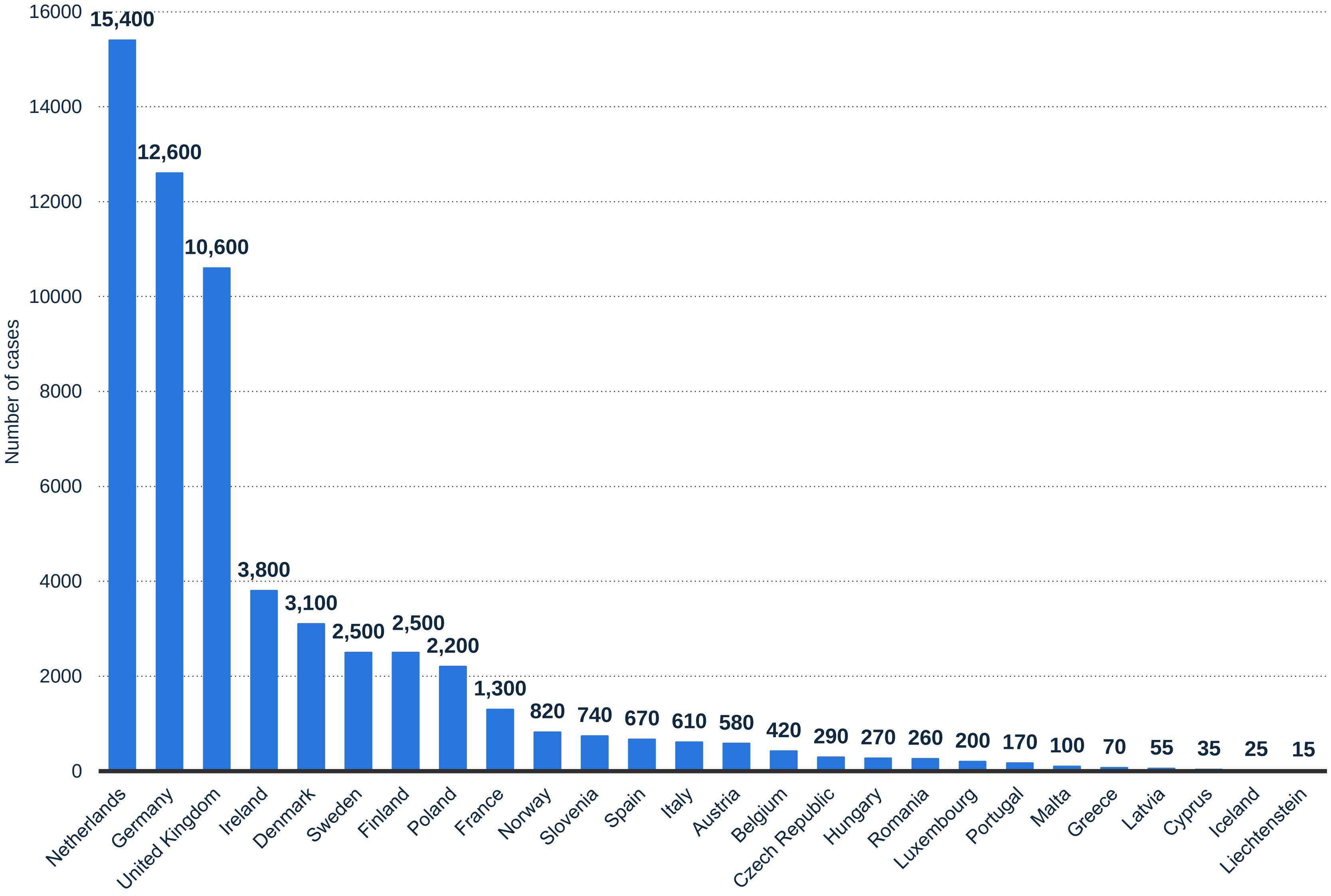
Main GDPR complaints in tech sector

GDPR complaints reported to the Irish Data Protection Commission 2018, by type



A breakdown of the GDPR complaints reported to the Irish Data Protection Commission (DPC) represents a significant overview of GDPR-related issues in the tech sector in the EU. In fact, the Irish DPC has jurisdiction over European complaints involving several multinational tech and digital groups (like Adobe or LinkedIn) that have their EMEA headquarters in Ireland. Since 2018, the activity of the Irish DPC has been increasing significantly. Between May and December 2018, the Irish watchdog received 2,864 complaints, an increase of 56 percent if compared to pre-GDPR activities. Among the reported cases of GDPR infringements, violation of access rights was the most common category, as well as unfair processing of data and data disclosure and complaints about electronic direct marketing.

Note: Ireland; May 25, 2018 to December 31, 2018
Source(s): Data Protection Commission



Data breaches in 2019 by country

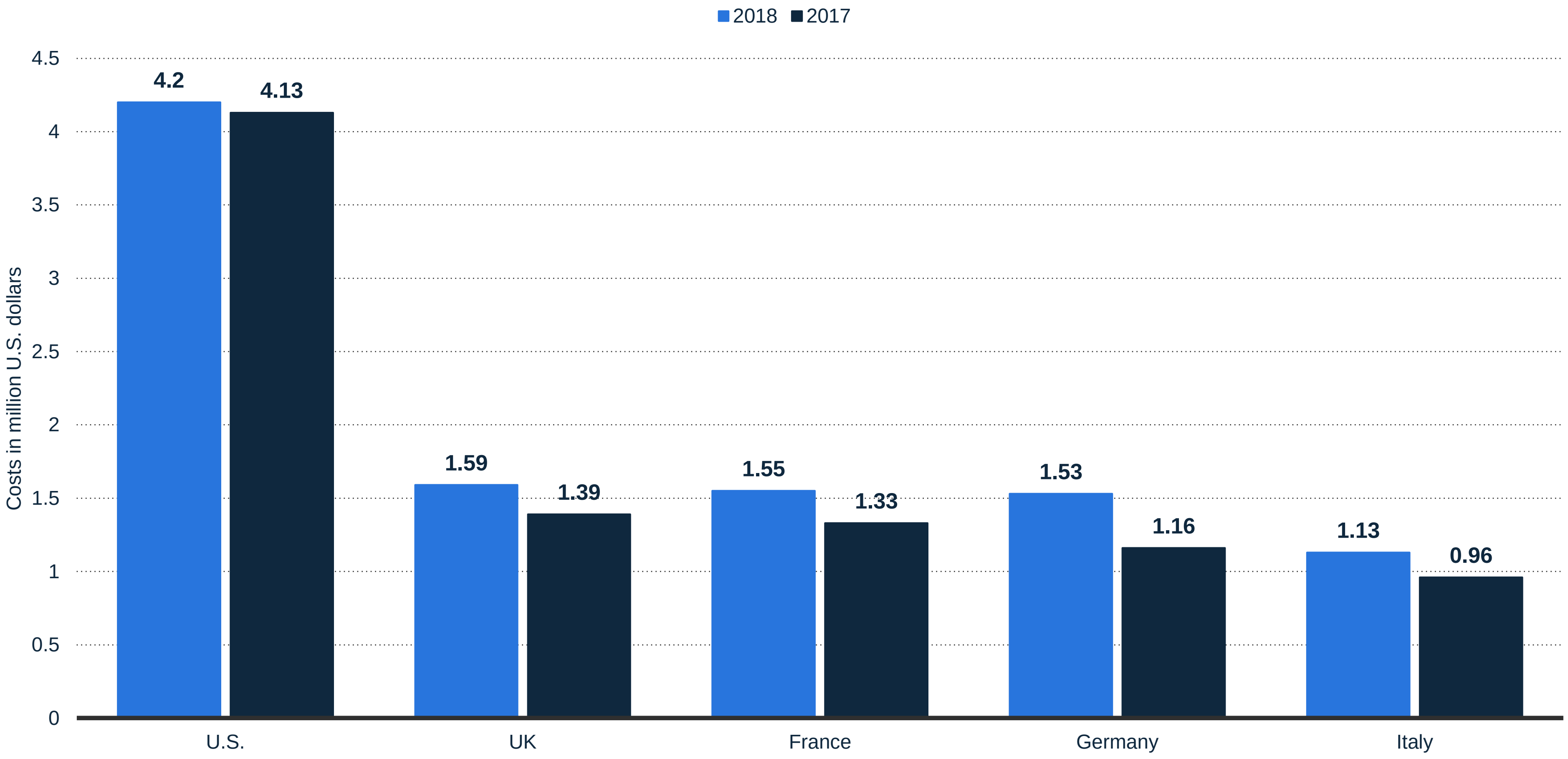
As mentioned on page 9, a significant amount of GDPR complaints consist in data breaches. Between May 2018 and January 2019, the international law firm DLA Piper estimated that about 60 thousand data breaches occurred in the EU. The Netherlands lead this ranking with 15,400 cases, mainly because the Dutch legislation on data protection has been quite strict even before the introduction of the GDPR. Further differences among countries are also due to different interpretation of the law lead by different jurisprudences.

Note: Europe; May 25, 2018 to January 28, 2019
Source(s): DLA Piper; Various sources (National data protection authorities)

The cost of data breaches

Estimated lost business costs due to data breaches in 2018 and 2017, by country (in million U.S. dollars)

Data breaches can cause loss of revenues, customers, and sometimes even brand reputation. In 2018, the lost business costs caused by data breaches increased compared to the previous year. Also, data breaches require allocating resources to other areas, like notification and detection of unauthorized data releases.



Note: Worldwide; 477 organizations and 2,200 individuals
Source(s): IBM

02 Challenges for enterprises

- Challenges of GDPR compliance
- Compliance impact
- Privacy professionals

The importance of being compliant

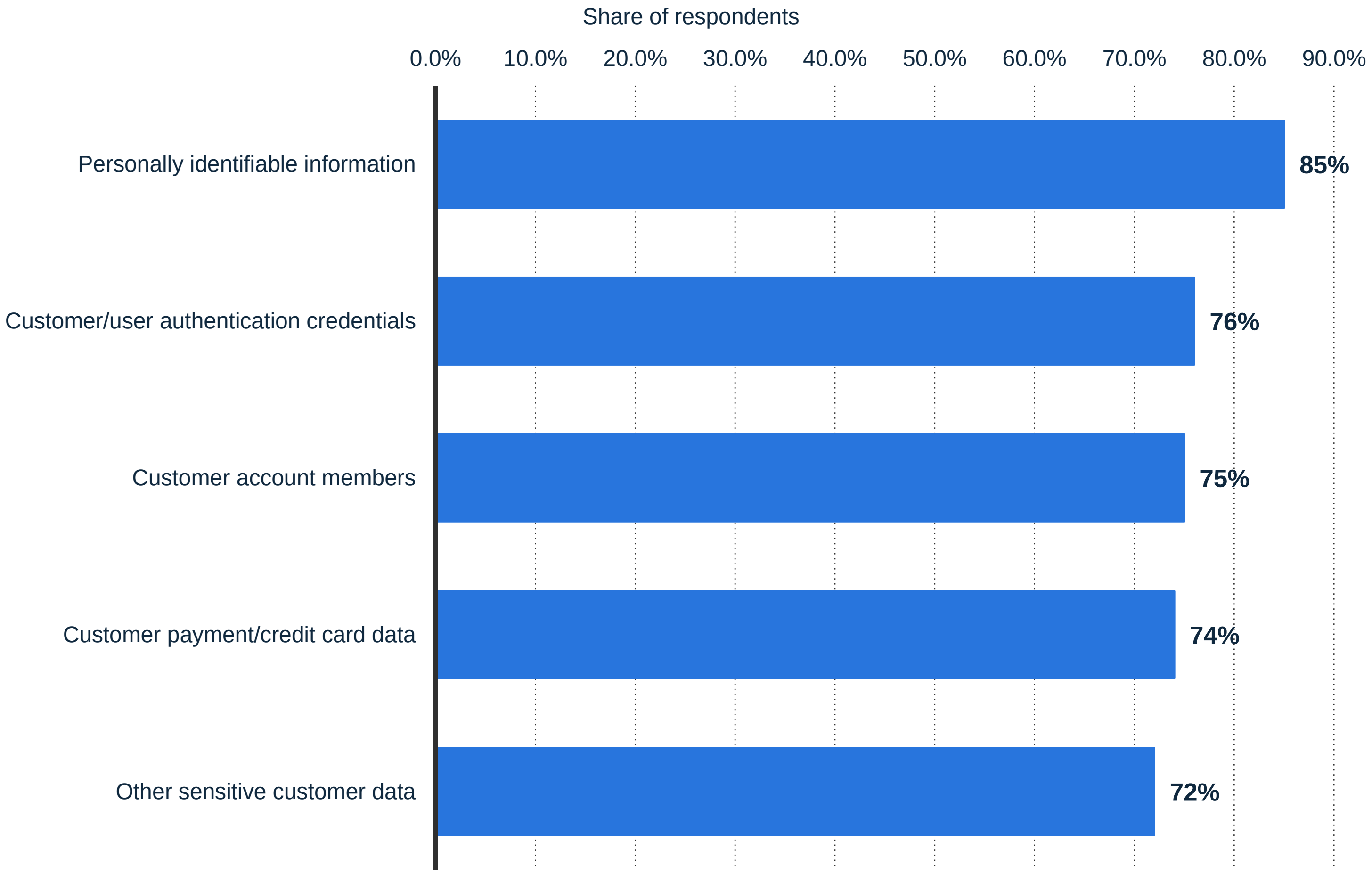
How data protection affected companies and the role of privacy professionals

Companies could have been better prepared for the GDPR: an IBM report from 2018 indicates that only 36 percent of companies worldwide expected to be fully compliant by May 2018. The presented insights suggest that the GDPR has been seen by enterprises as very complex and somewhat unclear in the concrete changes of business procedures. Companies might have waited to see the effective impact of the regulation, before investing internal resources in it. However, the regulation brought more internal transparency among European companies than the companies in the U.S. A study by the Ponemon Institute from 2018 indicated that 43 percent of European organizations audited their data on individuals to understand how data were used and where they were located. Only 29 percent of U.S. companies did the same. Companies achieved the new standards of data protection mainly to meet customers' requirements and protect their own brand reputation. Additionally, the privacy maturity level in companies affected selling processes, although with differences among countries and industries.

As mentioned on page 6 of this DossierPlus, the GDPR requires companies to employ a Data Protection Officer (DPO), responsible for data security auditing and training of the employees working on data processing. A Data Protection Officer must be an independent expert, who cannot operate influenced by business profits. Many companies working with data already had professionals responsible for data governance; quite often, in European companies, the so-called privacy leader worked also as a DPO. As a general trend, the International Association of Privacy Professionals (IAPP) predicts increasing demand of DPOs and privacy-related professional figures, especially in B2B businesses. The international recruitment agency Hays estimated that the demand for Data Protection Officers will increase to 75 thousand positions available worldwide in 2019.

What data do companies have on their customers?

Customer data held by companies in Europe 2018, by type of data

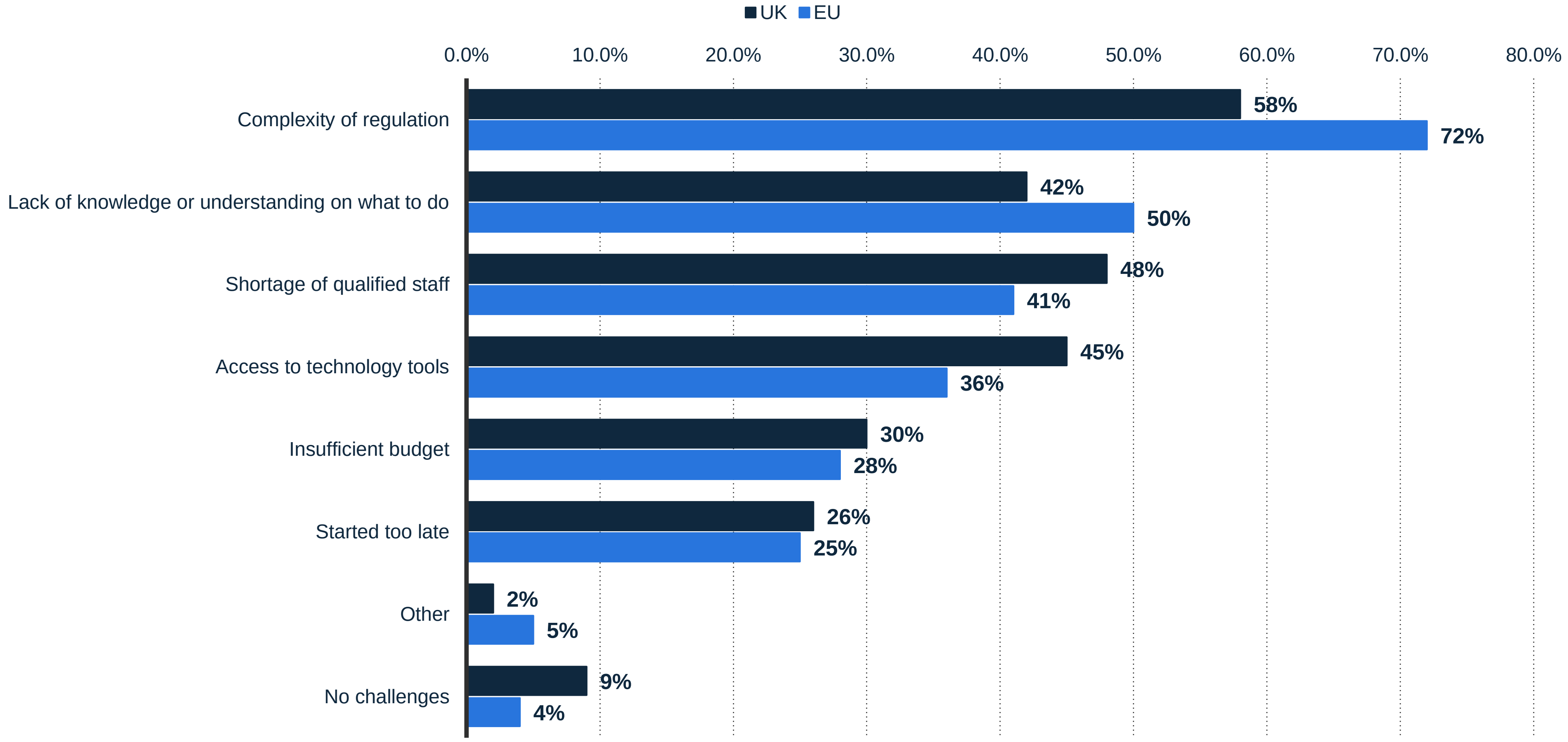


In a 2018 poll, 85 percent of European companies stated that they managed personally identifiable information related to their customers. The term – often indicated as PII – refers to any data that can be used to trace a person's identity. PII can be an individual's full name, address, social security number, passport number, etc. Another 72 percent of companies store other sensitive data, which are harder to define and depend on the industry. They might include intellectual property data, health-related data, and other industry-related specific information.

Note: Europe; March to April 2018; 5,878 Respondents; companies
Source(s): Kaspersky Lab

Main challenges of GDPR compliance among companies

Concerns about GDPR compliance among EU and UK companies

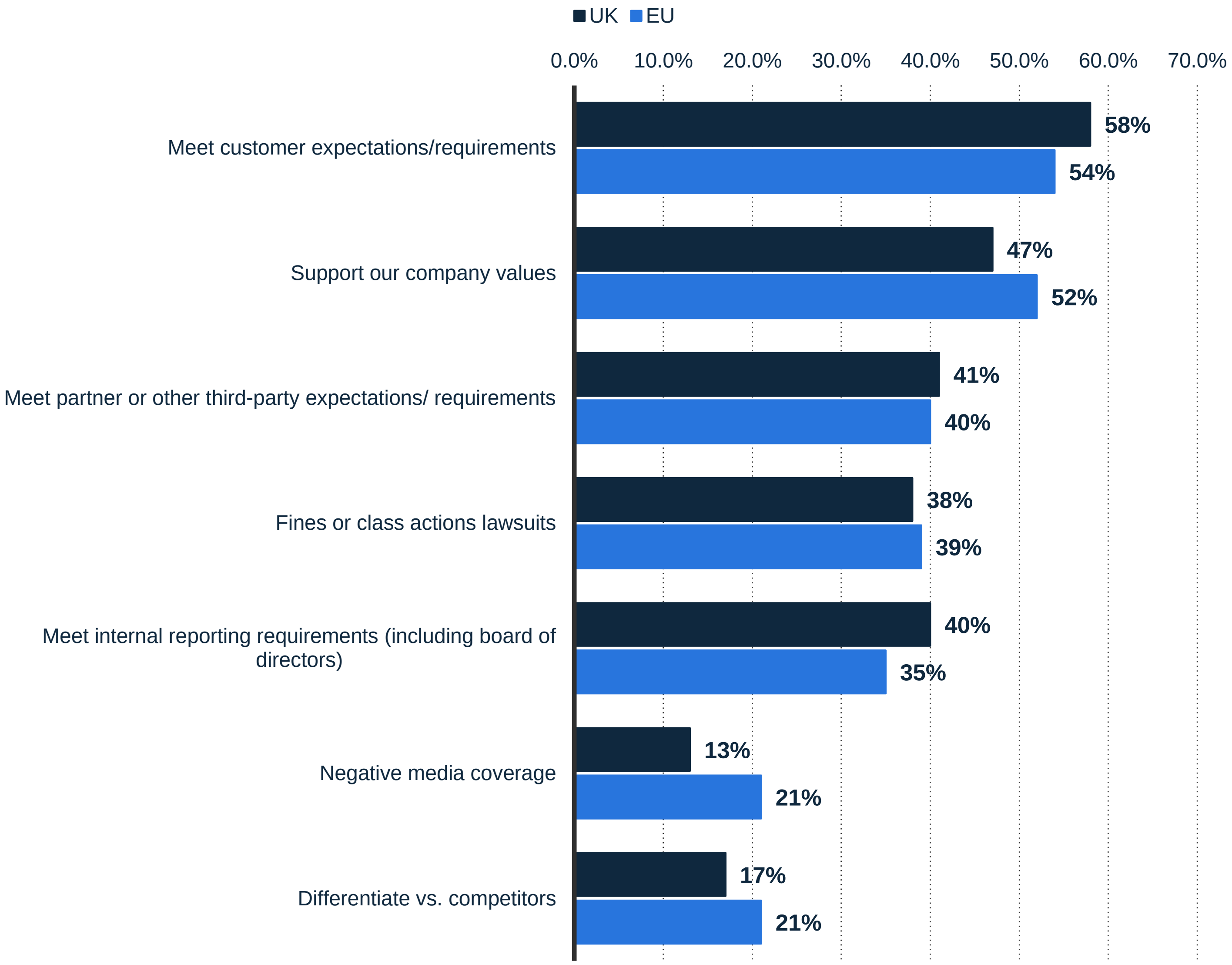


When implementing the GDPR compliance, 72 percent of professionals working in European companies were concerned about the complexity of the regulation, which required actions in different areas.

The lack of qualified staff was a challenge in 41 percent of European companies and 48 percent of the English ones.

Note: EU; June 4 to 15, 2018; +400 Respondents; 50 percent IT, 47 percent legal and 3 percent dedicated privacy professionals
Source(s): TRUSTe

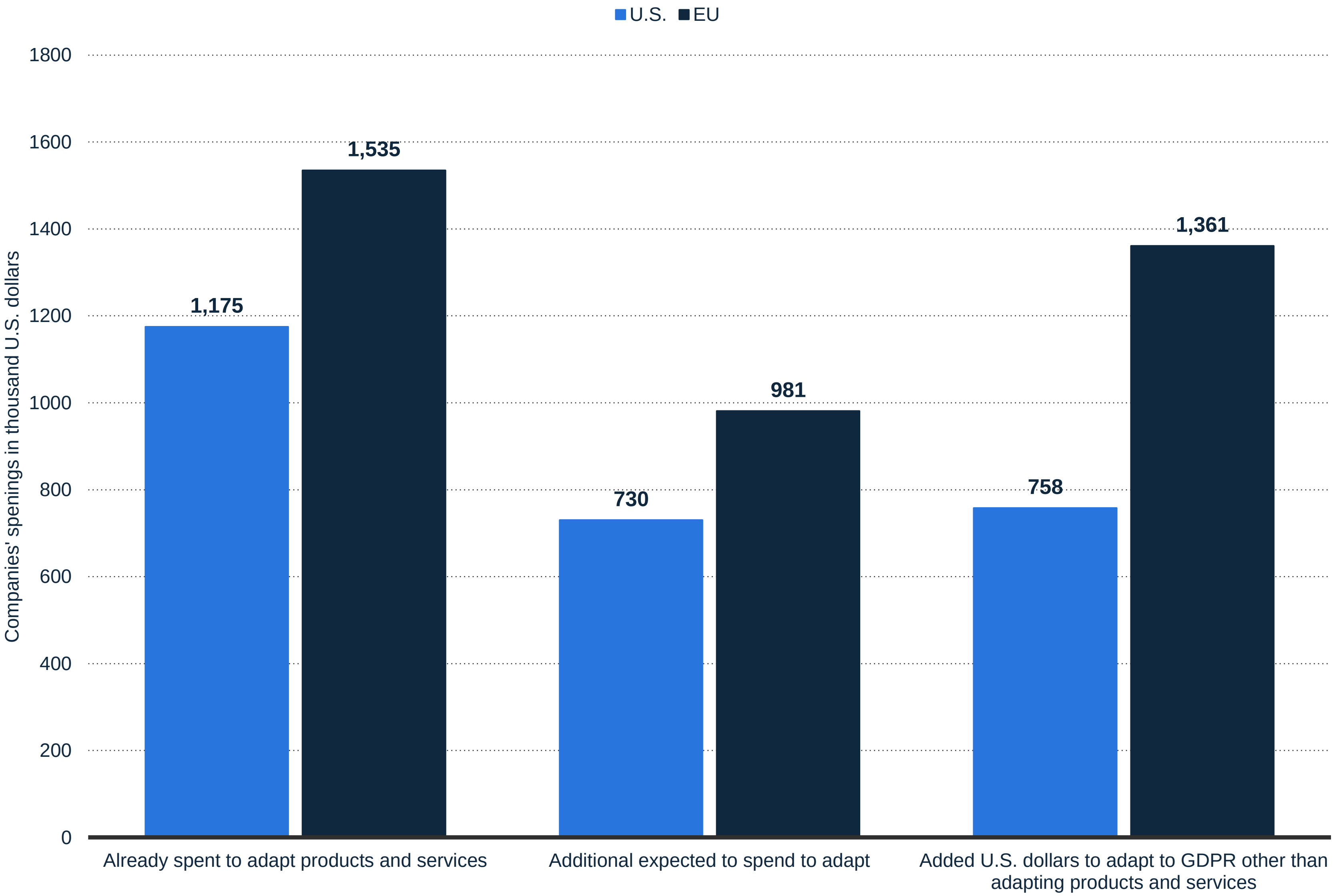
Main reasons to invest in GDPR compliance in 2018



The GDPR has a system of fines and penalties to disincentive data misuse, but this was not the main concern for European enterprises when it was first introduced. 54 percent of professionals in European companies and 58 percent of UK ones decided to invest in GDPR compliance to meet customer expectations or requirements, rather than to avoid financial penalties or class actions lawsuits. This may be influenced by the fact that the survey was conducted just after the GDPR's introduction, when penalties for violation had not been issued yet.

From 2019, the situation might change, as national authorities have acquired enough resources and expertise to investigate cases of non-compliance.

Note: EU; June 4 to 15, 2018; +400 Respondents; 50 percent IT, 47 percent legal and 3 percent dedicated privacy professionals
Source(s): TRUSTe



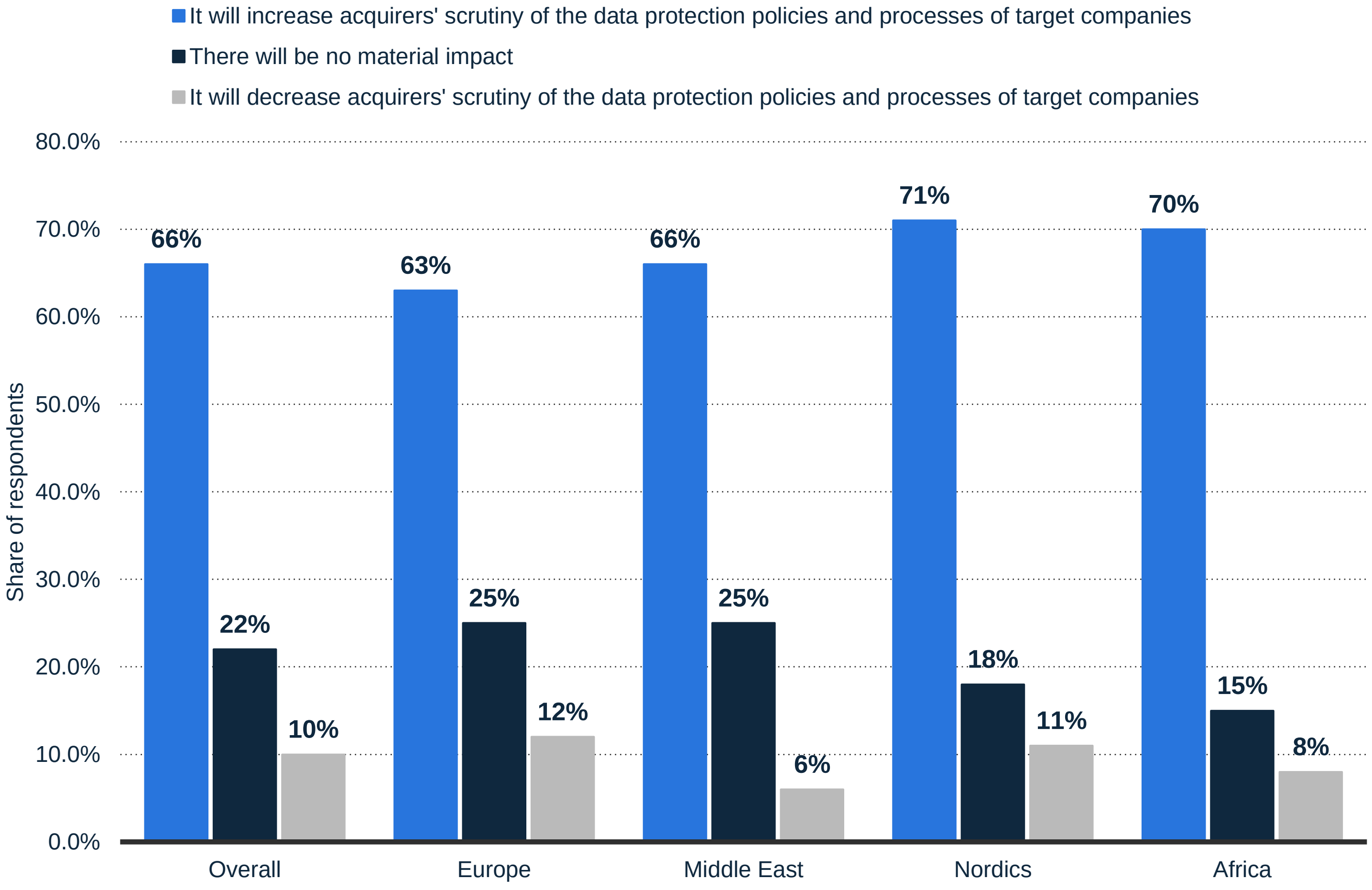
Spending on compliance in the EU and the U.S.

The displayed data shows the value of spending on GDPR compliance among companies where privacy professionals operate. In 2018, the average spending was higher in the European Union, with about three million U.S. dollars spent annually. After May 2018, further investments were expected but in lower amounts. After the GDPR introduction, resources are allocated only to maintain regular privacy controls and monitor data inventories.

Note: United States, EU; 2018; 550 Respondents
Source(s): EY; IAPP

Future GDPR impact on M&A due diligence

In the next five years what impact do you expect the EU’s GDPR to have on M&A due diligence?

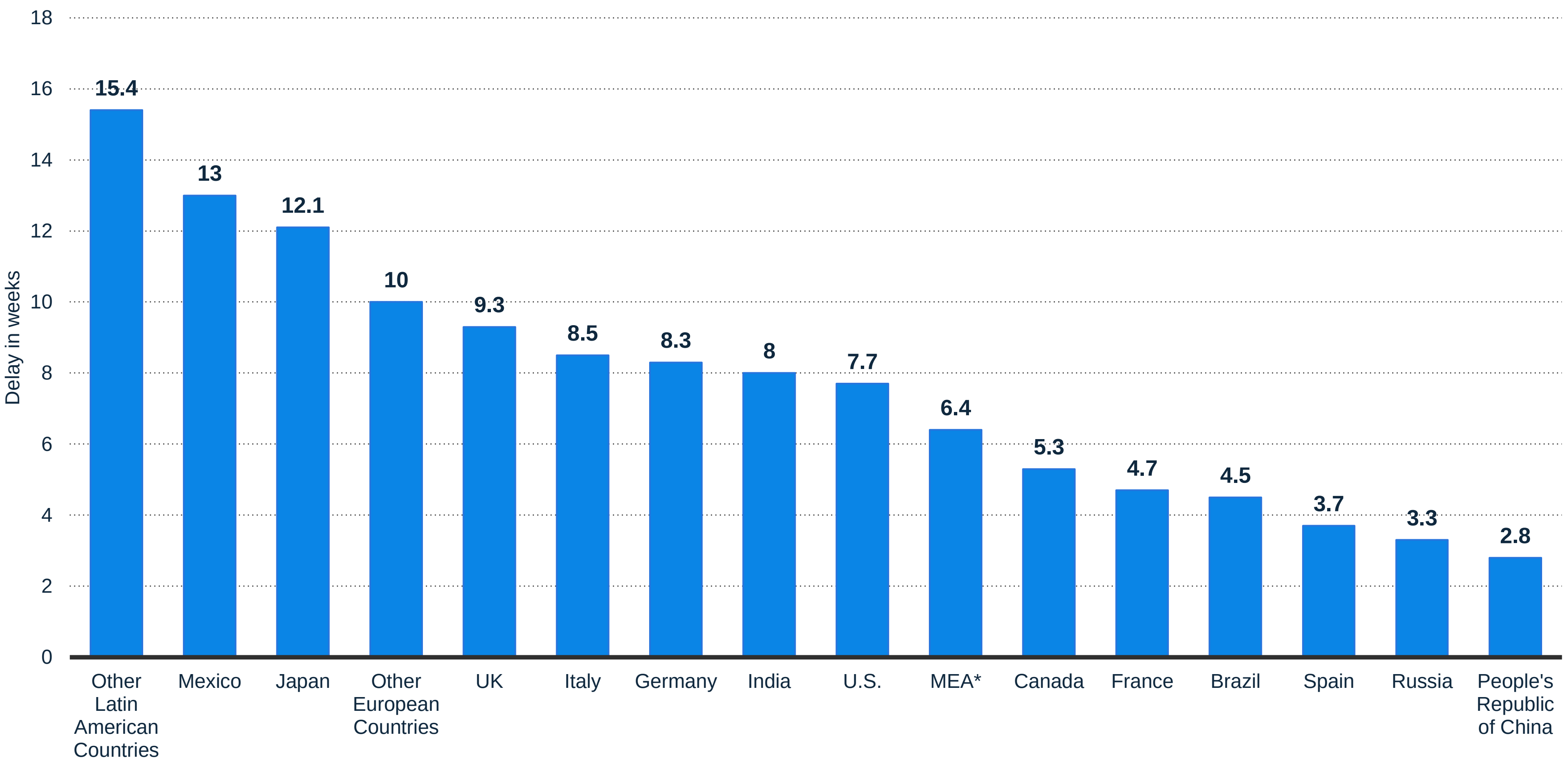


In next five years, compliance to the GDPR will be a time- and resource-consuming operation regarding due diligence of mergers and acquisitions. Due diligence means the gathering of information about investment’s risks. According to professionals working in the EMEA region, employees and consultants of acquirers will examine data policies of companies to a greater extent.
In the same survey shown here, 55 percent of professionals reported to have worked on transactions that had to be terminated due to concerns ~~regarding~~ data protection.

Note: Europe; July 2018; 539 Respondents; professionals involved in M&A transactions in the EMEA region
Source(s): Merril Corporation;

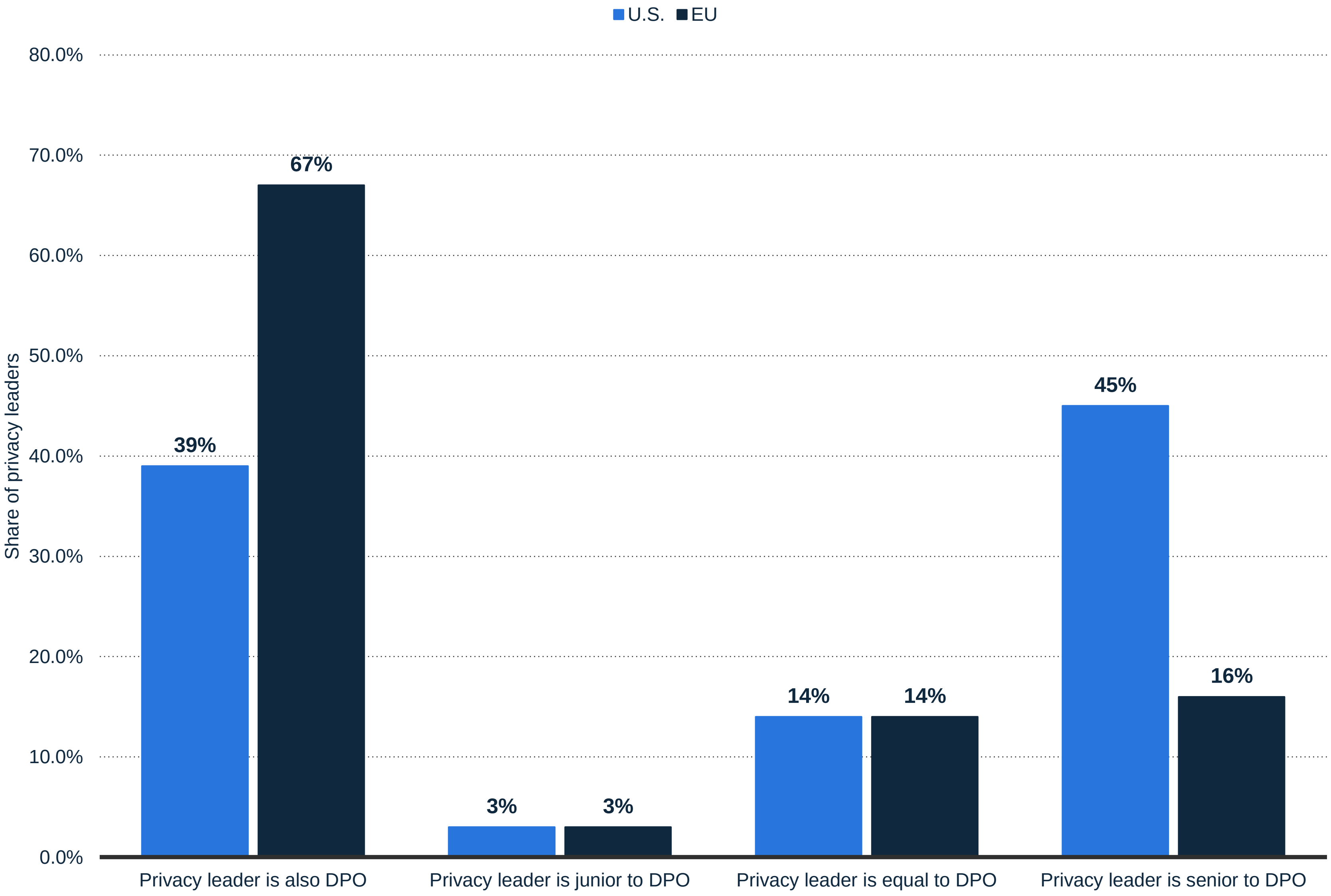
EU regulation pushes sales delays

Average number of weeks of sales delay due to privacy requirements in 2018, by country



Across the shown countries, the compliance to privacy regulations causes delays in the selling cycle. In Latin American countries, the sales delay is greater than in the EU and the U.S. Two main reasons behind the delays were the investigation of specific requirements and the translation of policies into other languages.

Note: Worldwide; 2018; 2,992 Respondents; Sale managers
Source(s): Cisco Systems



Privacy professionals: Data Protection Officer as privacy leader in the company

Under the GDPR, data controllers must appoint a Data Protection Officer. In European companies, the person responsible for privacy decisions in a company before the GDPR would often cover the position of Data Protection Officer. In the U.S., where the expected impact of the GDPR is lower, the Data Protection Officer tends to be someone in charge, while in 45 percent of cases, the privacy leader is senior to the DPO.

Note: United States, EU; 2018; 500 Respondents
Source(s): EY; IAPP

03 Data driven marketing

- Privacy policies on websites
- Online traffic and ad vendors
- Third-party tracking

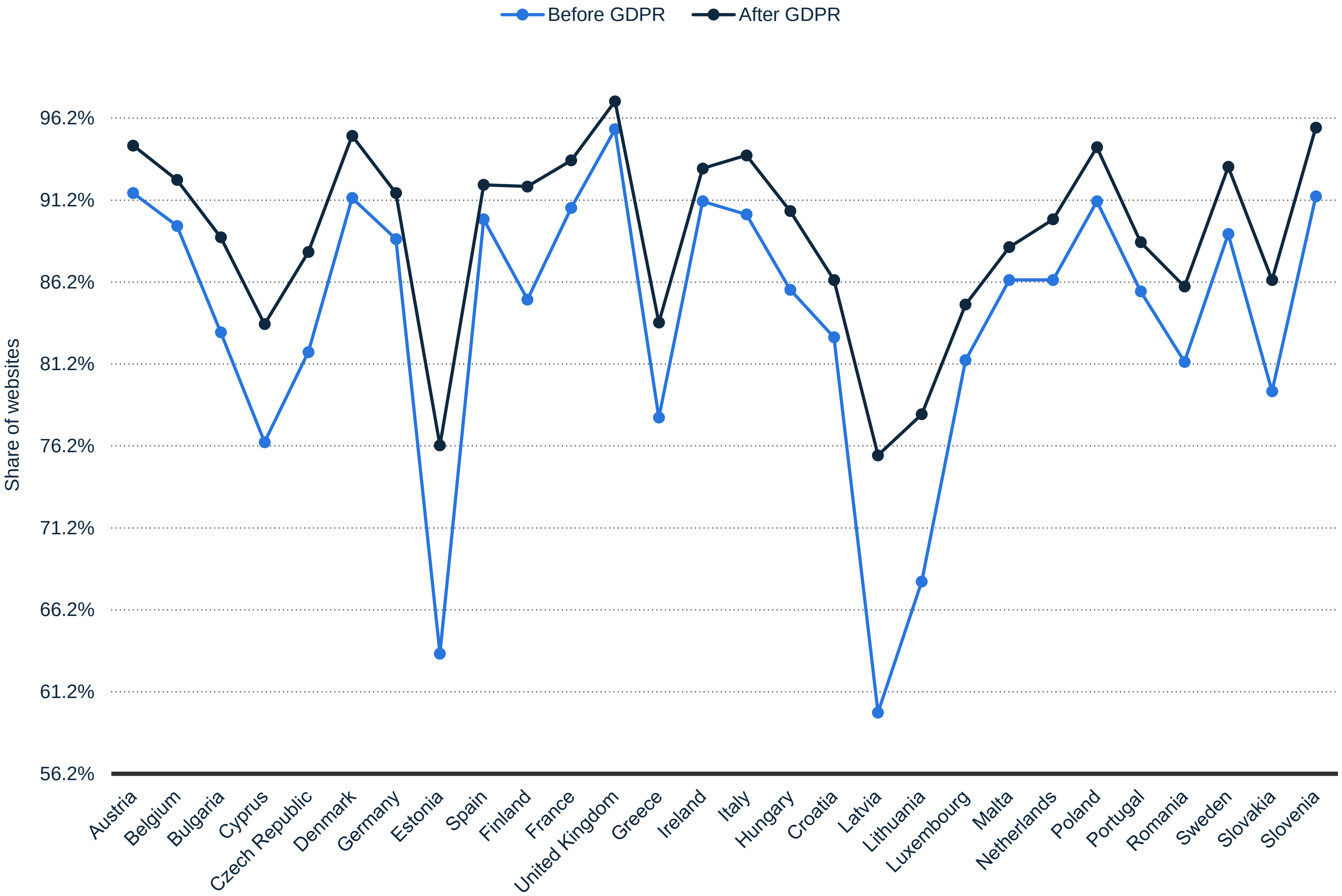
Trouble in marketing heaven

How the GDPR affects data-driven marketing

Due to the GDPR, website publishers had to establish a concrete legal basis for processing user data. As a result, the number of privacy policies uploaded online has significantly increased. Apart from this requirement, the regulation affected data-driven advertising displayed on sites. As of May 2018, the number of GDPR-compliant websites where ads could be displayed was very limited but started to increase, as Smaato's data on ad spending showed for the mobile market.

One immediate result of the GDPR has been a reduction of trackers set by small vendors, while Google's presence remained stable. In 2019, Google's alignment to the GDPR evolved and the tech giant decided to join the TCF, the Transparency and Consent Framework set by the International Advertising Bureau Europe (IAB), which had been already launched in 2018. The aim of the TCF is to have a transparent tool through which publishers and vendors can gather user-data and ensure users' access to their data. The performance of ad vendors after Google's commitment will be assessed in the second half of 2019, when Google is expected to reach a final agreement with the IAB on the TCF's update.

In post-GDPR programmatic marketing, online tracking will continue to be more difficult for third-party data trackers and enhance the role of first-party trackers. First-party cookies are controlled only by the site owner and are set for internal analytics or to facilitate the user experience; first-party trackers are less impacted by privacy settings, as online visitors are identified but usually stay anonymous. By contrast, users tend to opt-out of allowing third-party cookies more frequently, often through browser settings. Besides, third-party cookies might be altered when users browse anonymously. As marketers struggle to obtain the explicit users' consent for retargeting (see glossary), companies that have the resources will profile customers through their own online channels. Some enterprises will focus on the data that matter, through more control over their own customers' information.



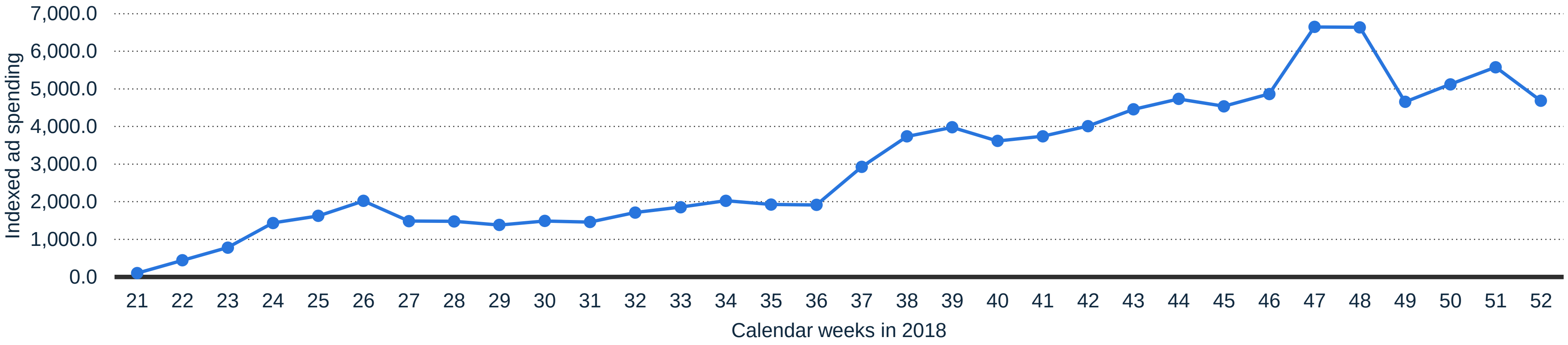
Most popular websites with privacy policies before and after the GDPR

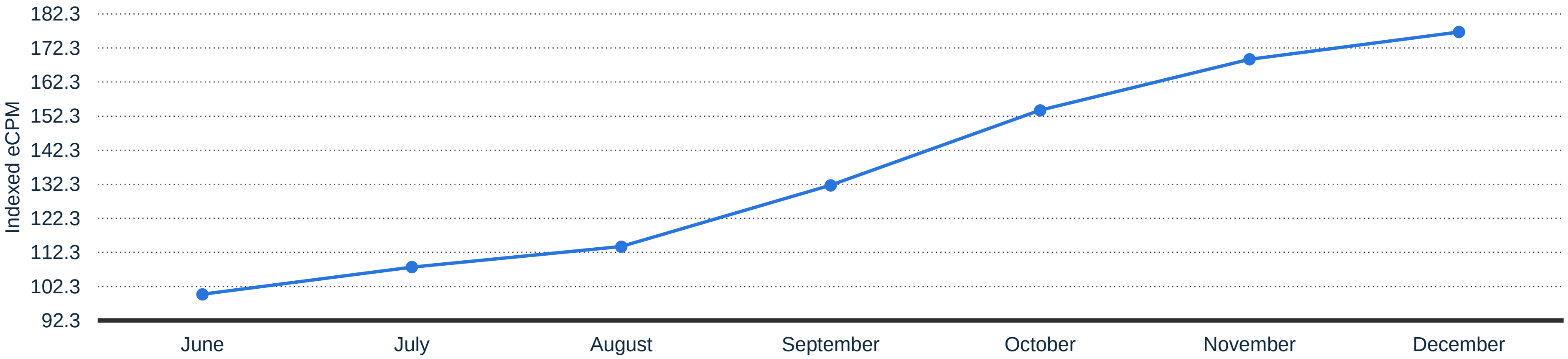
This graph shows the share of the most popular websites with privacy policies available before and after the GDPR's introduction. The study takes into consideration the 500 most frequently visited websites in each EU country. After May 2018, a greater number of websites added privacy policies to inform the visitors about the users' data processing. Across the EU, the GDPR enforced transparency regarding data treatment online.

Note: Europe, EU; December 2017 and October 2018
Source(s): Uni Bochum

Mobile ad spend and effective cost-per-mille after May 2018

Mobile ad spend for impressions with GDPR consent and monthly eCPM in Europe



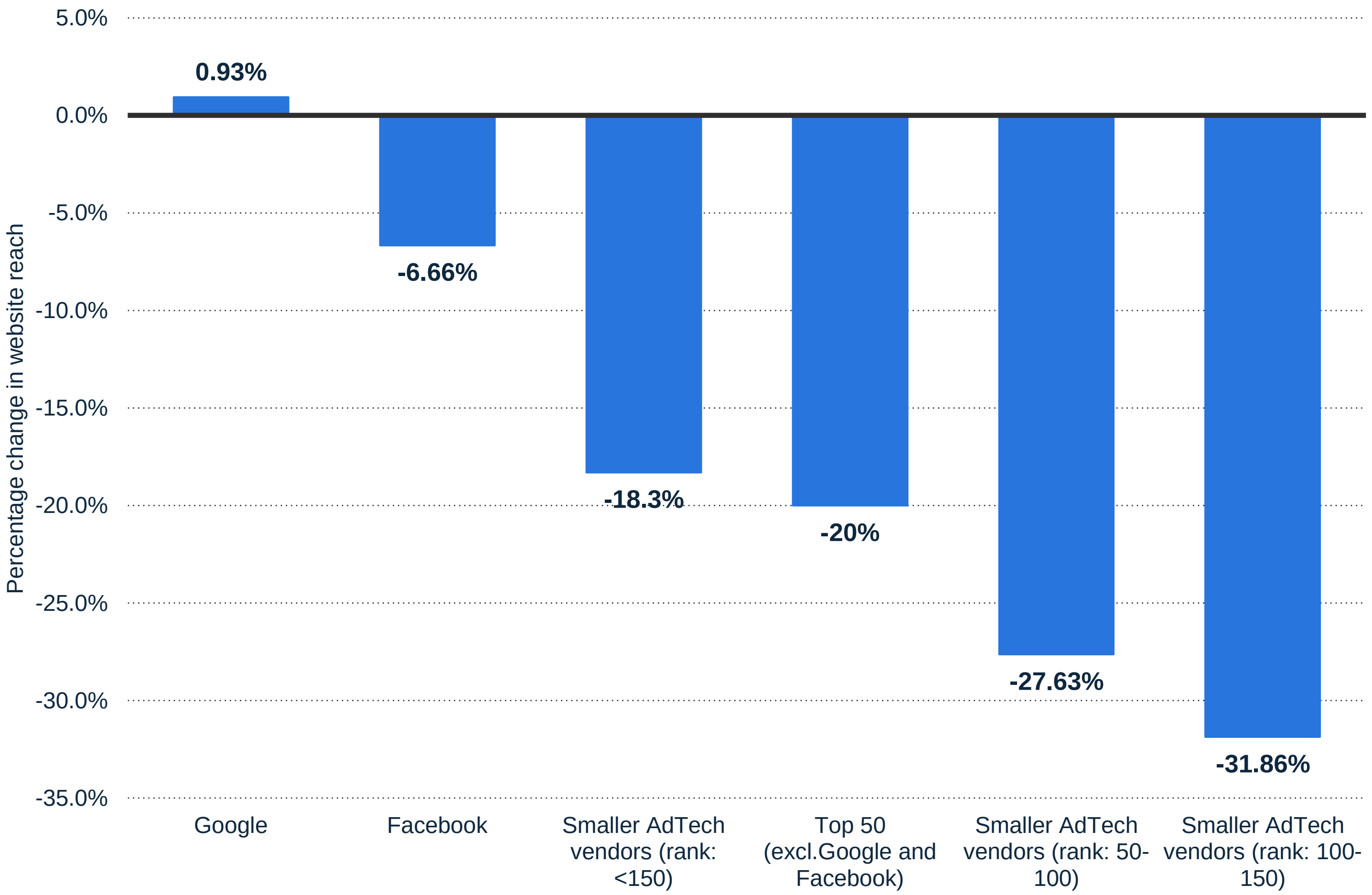


According to Smaato, after May 2018, the supply of GDPR-compliant impressions was limited and the ad spending was low. Afterwards, more inventory from GDPR-compliant sites was made available through renewed users' consent. Programmatic investments by advertisers gradually increased again. This produced a growing effective cost-per-mille.

Note: Europe; H2 2018; on Smaato Publisher Platform (SPX)
Source(s): Smaato

Website reach of advertising vendors

Percentage change in website reach of advertising vendors in Europe in 2018



Small ad vendors lost traffic

This graph shows the lost web reach of small ad vendors* due to the GDPR. After May 2018, publishers of websites could not track users for advertising as much as before. Therefore, trackers of ad vendors reported decreasing online traffic volumes. Small ad vendors might have had lesser resources to invest in GDPR compliance, compared to big tech giants like Google or Facebook. In 2018, online ad campaigns delivered through Google could follow users through up to 12 trackers, including Google. This limited number of web trackers excluded all other tracking tools provided by smaller ad vendors, reducing competition in digital advertising. The following insights show the websites most affected by the trackers' drop.

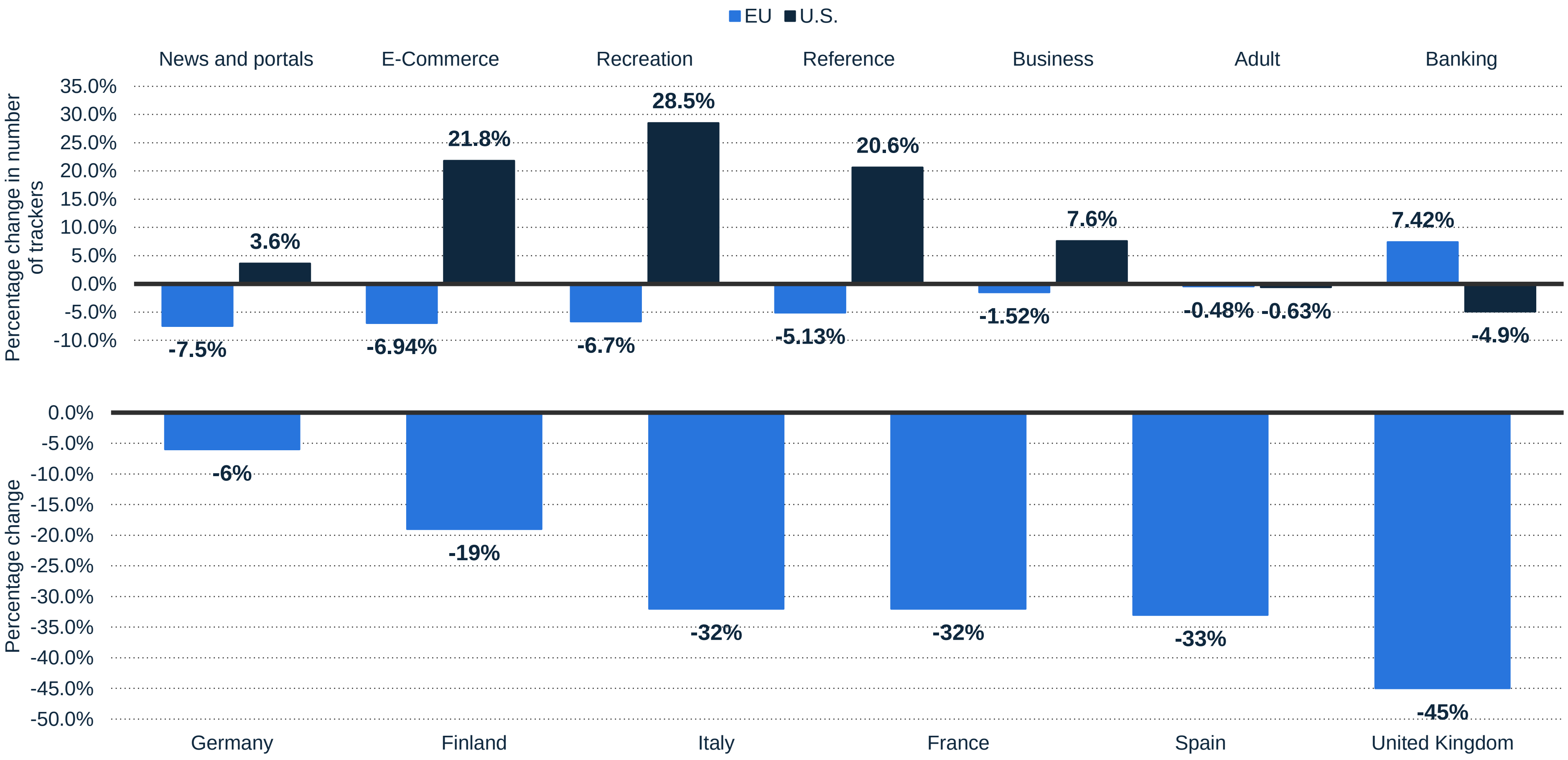
*Vendors' rank is based on the reach of the vendors' trackers. In this statistic, the analysis made by Cliqz through the whotracks.me platform takes into consideration 200 advertising services. The rank is calculated taking into several factors regarding the presence on the web pages and the frequency with which trackers are loaded.

Note: Europe; April to July 2018

Source(s): Cliqz

Cookies per page: most affected websites and countries in 2018

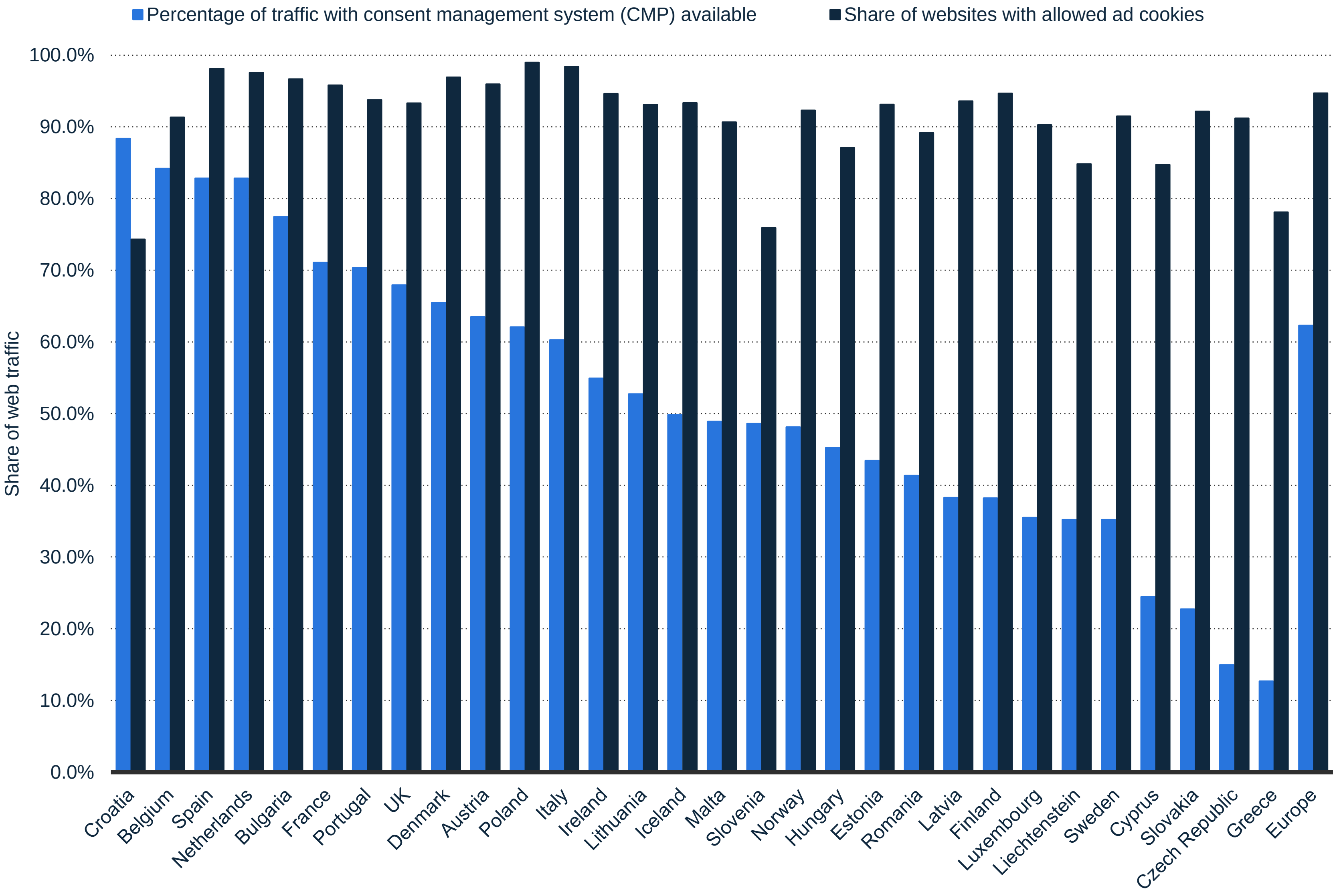
Change in number of trackers per page on websites by type and on news sites by country



In the EU, news sites and portals lost the highest number of trackers. In fact, compared to other categories, news sites usually display a lot of ad trackers to generate revenue. The second graph shows the decreasing number of third-party cookies on news sites in selected European countries.

Note: North America, Europe; April to July 2018
Source(s): Cliqz

Note: Europe; April and July 2018
Source(s): Reuters Institute for the Study of Journalism



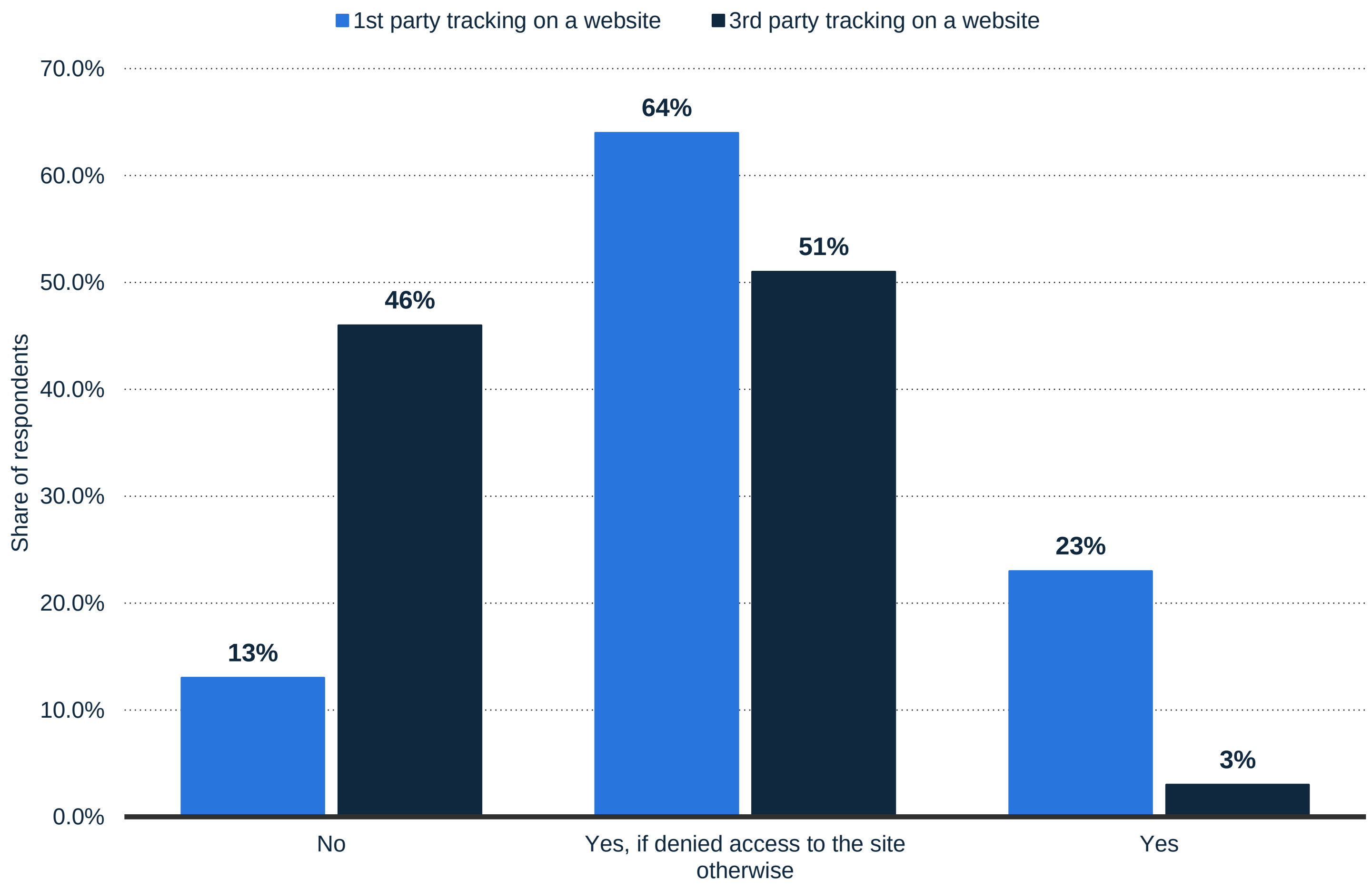
Web traffic with consent management systems

Websites publishers collect user consent through consent management tools (CMPs). CMPs existed already before the GDPR but tended to be pop-up boxes rather than opt-in forms. In November 2018, data showed that consent management systems were provided on 64 percent of European websites. Users tended to largely consent to online tracking for personalized advertising purposes.

Note: Europe; 2018
Source(s): Teads

Expected users' consent in ad tracking

Do you believe that users will opt-in to tracking for the purposes of advertising?



When a consent framework is available, users tend to agree to targeted ads, as mentioned on page 26 of this dossier. But this also depends on who processes the data, according to a PageFair survey conducted among ad tech vendors and website publishers in 2017.
User behavior on websites can be tracked for advertising purposes by first-, secondary-, and third-party data (see glossary). Third parties provide companies with data to reach target-relevant consumers. For their trackers, the opt-in percentage is expected to be lower than first-party trackers. Third-party cookies present more risks for data privacy, as personal data is managed by different actors through many channels. Therefore, users might disable them completely through blocking services. By contrast, users are expected to opt-in easier to first-party tracking. First-party tracking is activated by the same domain’s owner, so the purpose of online tracking is more likely to be transparent.

Note: Worldwide; 2017; 305 Respondents
Source(s): PageFair

04 Current and future trends

- Data masking & data platforms
- The next ePrivacy Regulation

statista

Where are we going?

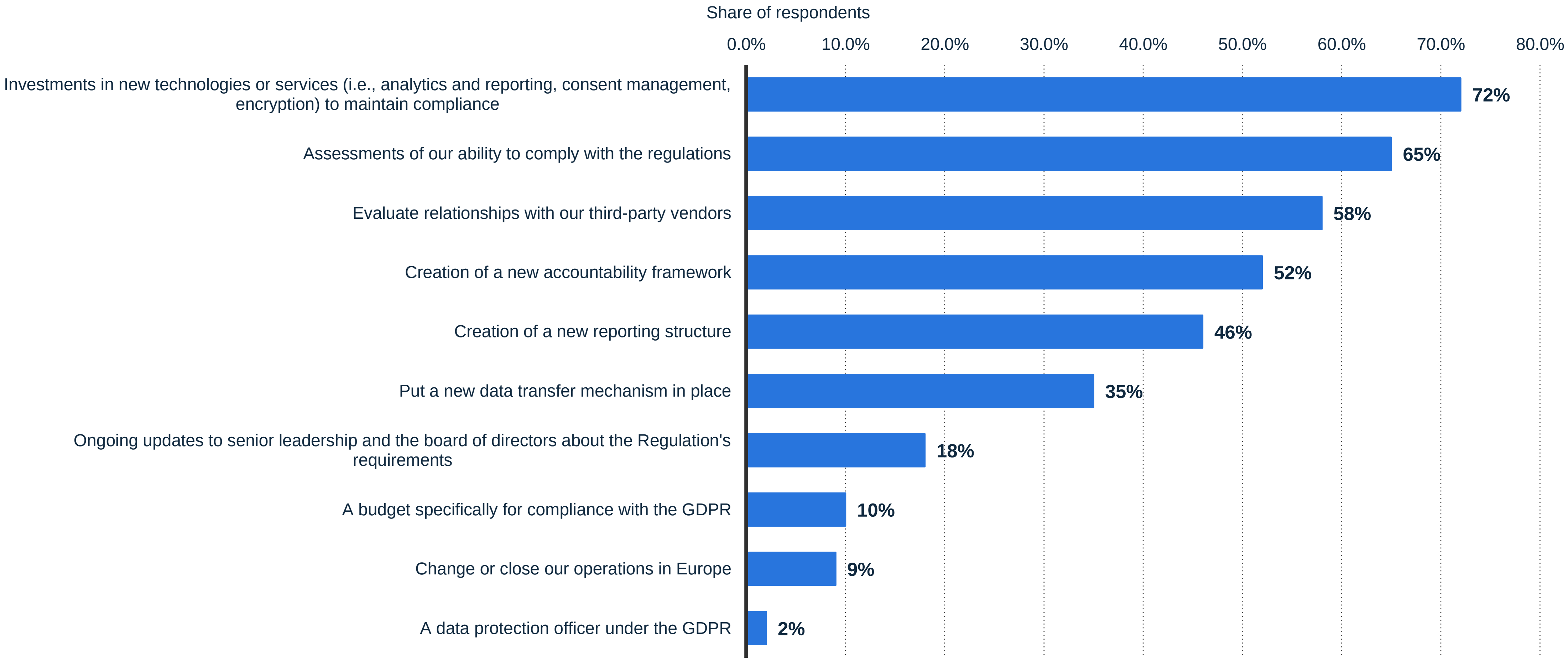
The GDPR principles were a template for other regulations, like the California Consumer Privacy Act and the Personal Information Security Specification in China, both issued in 2018. However, the European regulation seems far from being perfect: the Center for Data Innovation strongly recommends a reform of the GDPR, based on the significant compliance costs that would kill digital startups. The Center’s experts claim that the GDPR is too complicated for users and companies and hurts the AdTech industry. But the GDPR is here to stay. Also, it gave start to a proper *compliance industry*, with an expected market value of 1.19 billion U.S. dollars by 2023.

This chapter portrays some side opportunities offered by the GDPR’s enforcement. The shown insights are related to market segments companies would invest in, in order to avoid risk of non-compliance. To assess risks regarding data protection, companies need to know everything about the collected data. Therefore, customer data platforms (CDP) will be essential tools to gather fragmented data about customers, often stored in different cloud databases. According to the insights from the Customer Data Platform Institute, the European CDP’s market generated 230 million euros in revenues in 2018, with European vendors earning about 150 million euros. In 2019, the market growth rate is expected to reach 40 percent. The future growth trend will depend on the general use of cloud technologies (most CDPs are cloud-based), but the market is likely to grow faster in Europe than elsewhere. No standard procedure can ensure full GDPR compliance, but companies will implement further measures to safeguard data. This chapter shows the main drivers in common procedures, like data pseudonymization and encryption. Unlike safe data record keeping, pseudonymization and encryption are not mandatory under the GDPR. But their use is highly suggested to limit damages caused by potential data breaches. The two measures are different, though: pseudonymization removes personal data which identifies individuals, while encryption transforms personal data into a code.

Rules on data protection don’t end with the GDPR. By 2020, the European Commission should agree on the final draft of the ePrivacy Regulation. This regulation will require stricter but more user-friendly cookie settings, which will have a significant impact on web traffic, as the presented data suggest. Further, the ePrivacy Regulation calls for safety measures when collecting data processed through IoT technologies, by OTT and messaging services, and on metadata (contextual data related to any data activity).

Next key operations of companies after the GDPR introduction

A survey asked EU and U.S. professionals: which areas will require significant efforts after May 25?

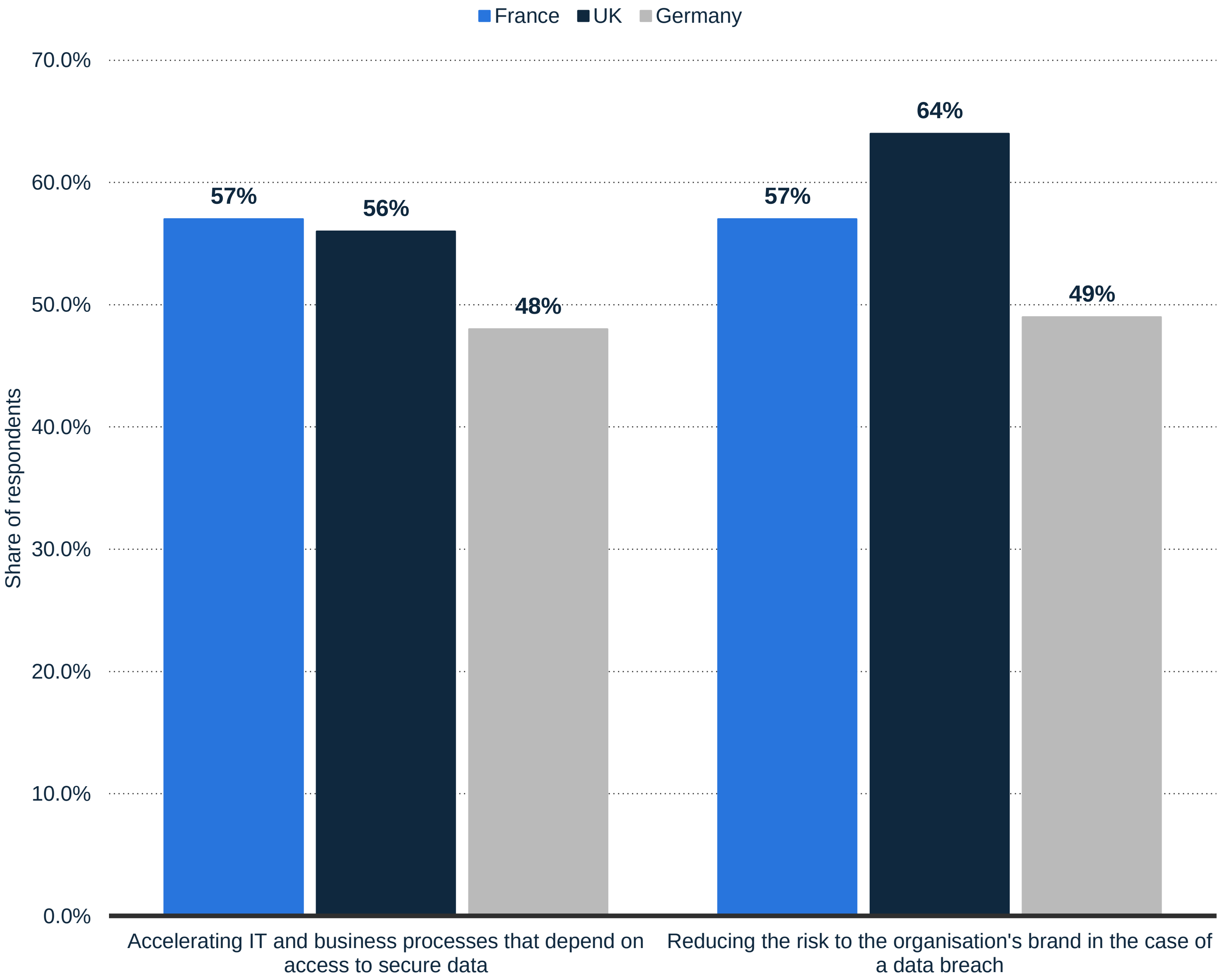


Note: United States, EU; 2018; 1,000 Respondents; IT and legal professionals working in companies
Source(s): McDermott Will & Emery

Reasons to use data masking

The GDPR encourages data processors to use pseudonymization methods to avoid identifying individuals directly. Therefore, the regulation might have a positive impact on the use of data-masking technologies. A Delhix survey from 2016 indicated that companies in the UK, Germany, and France planned to mask more of their stored data due to the GDPR over the following two years. In 2016, the estimated percentage of masked data (not including production data of the company) was expected to double by 2018. According to Market Research Future, the European data masking market is expected to increase, with Germany, France, and the UK highly investing in encrypting technologies. Globally, the market is expected to grow at 12 percent CAGR, and reach 830 million U.S. dollars by 2023.

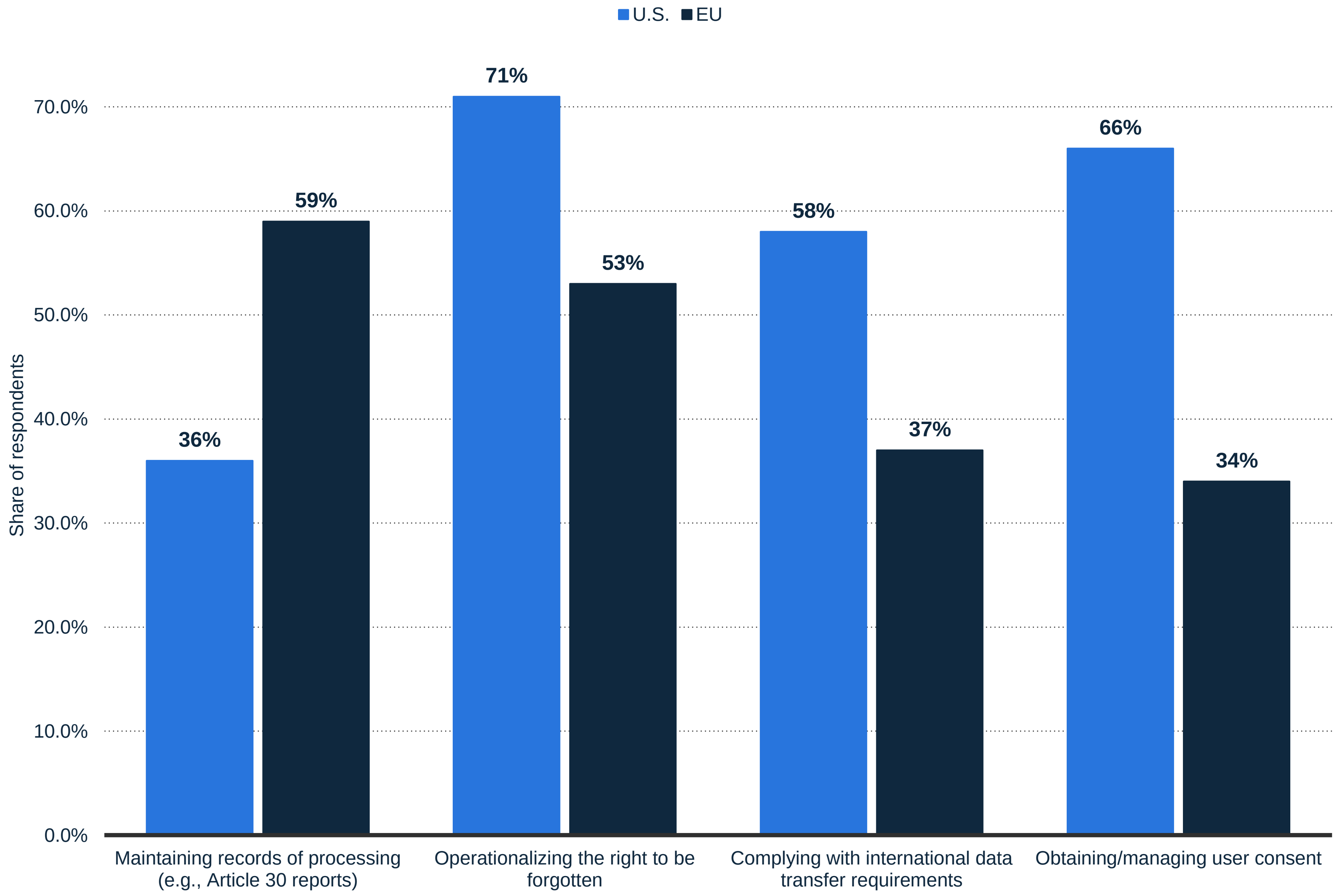
Pseudonymization can be achieved also through data encryption. By doing so, personal data is translated into a code, which can be read only through a decryption key. In case of an incident where data records are compromised, encryption solutions proved to be useful. A global study by Ponemon Institute showed that the extensive use of encryption was the second-most cost-saving factor in case of a data breach incident.



Note: France, Germany, United Kingdom (Great Britain); 2016
Source(s): Delphix

Biggest risks under the GDPR: keeping data records

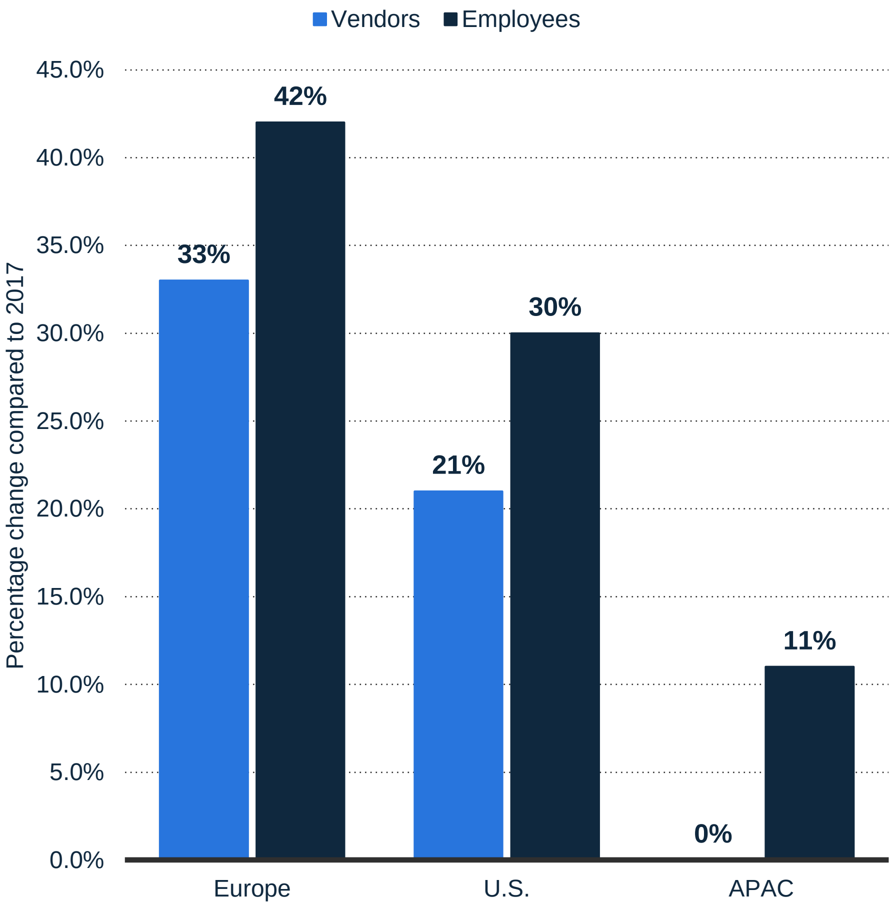
In Europe, the biggest risk of achieving compliance to the GDPR is keeping records of processed data. Not only do companies and organizations need to know exactly what kind of data they hold and where, but they are also required to store them safely in electronic records.
The GDPR forces them to keep big data sets organized, which is a time-consuming operation. In large companies, organized and clearly labeled data is an asset of higher potential value.

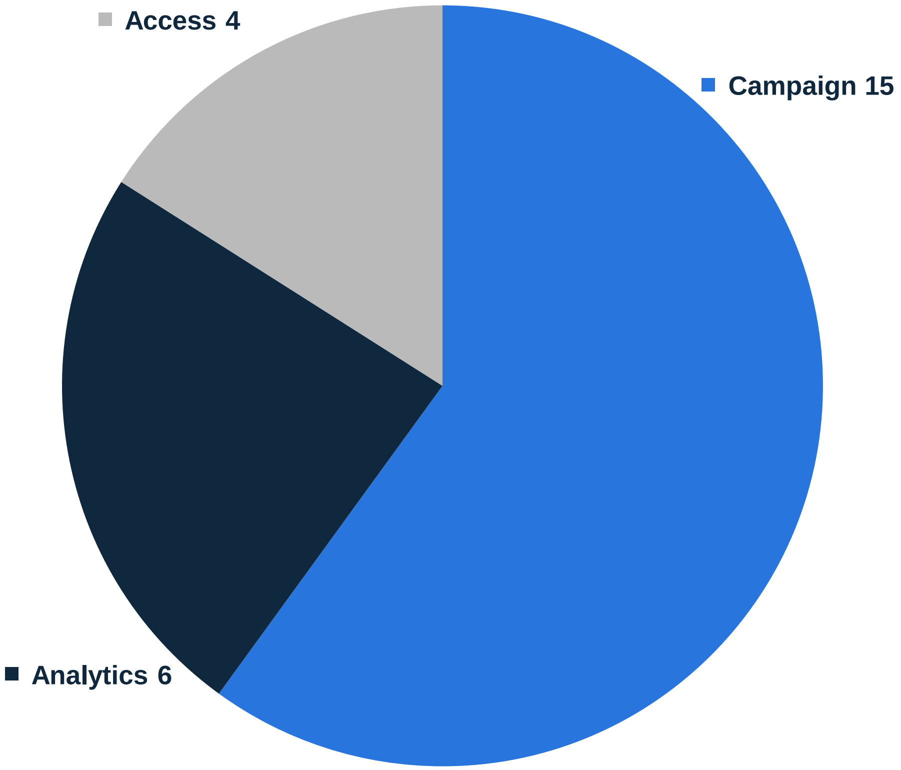


Note: United States, EU; 2018; Ca. 1,000; Companies
Source(s): McDermott Will & Emery; Ponemon Institute

Data protection makes customer data platforms grow

Growth in vendor & employee numbers at Customer Data Platform companies in 2018, and breakdown of EU vendors



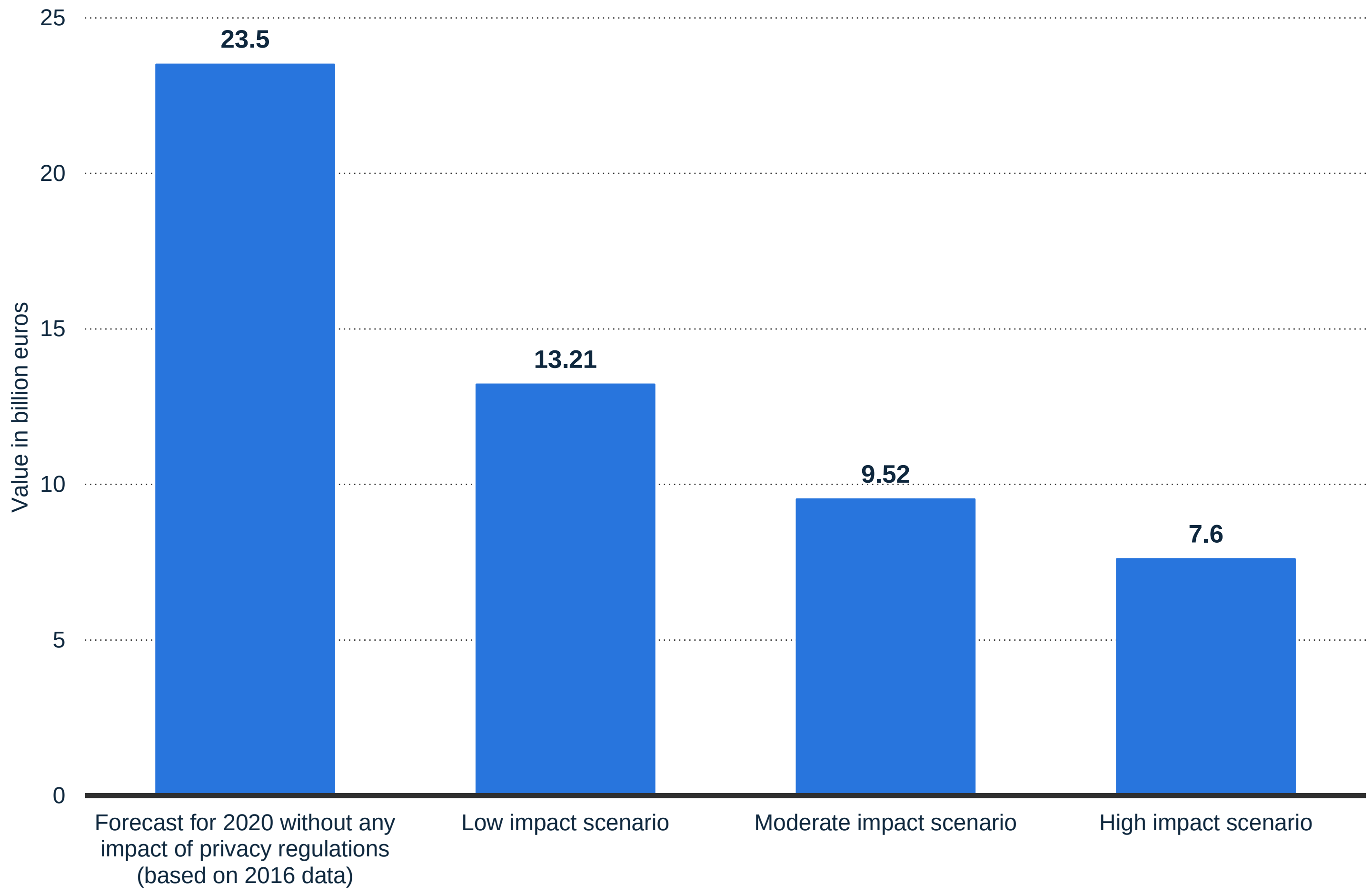


Compliance with data protection fostered the European customer data platform industry. Compared to 2017, the growth rates in the number of vendors and employees in the EU were significantly higher. Most vendors offer data management technologies for ad campaigns. This indicates that CDPs are useful especially for marketing activities.

Note: January to June 2018
Source(s): CDPInstitute.org

The next ePrivacy Regulation affects online targeting

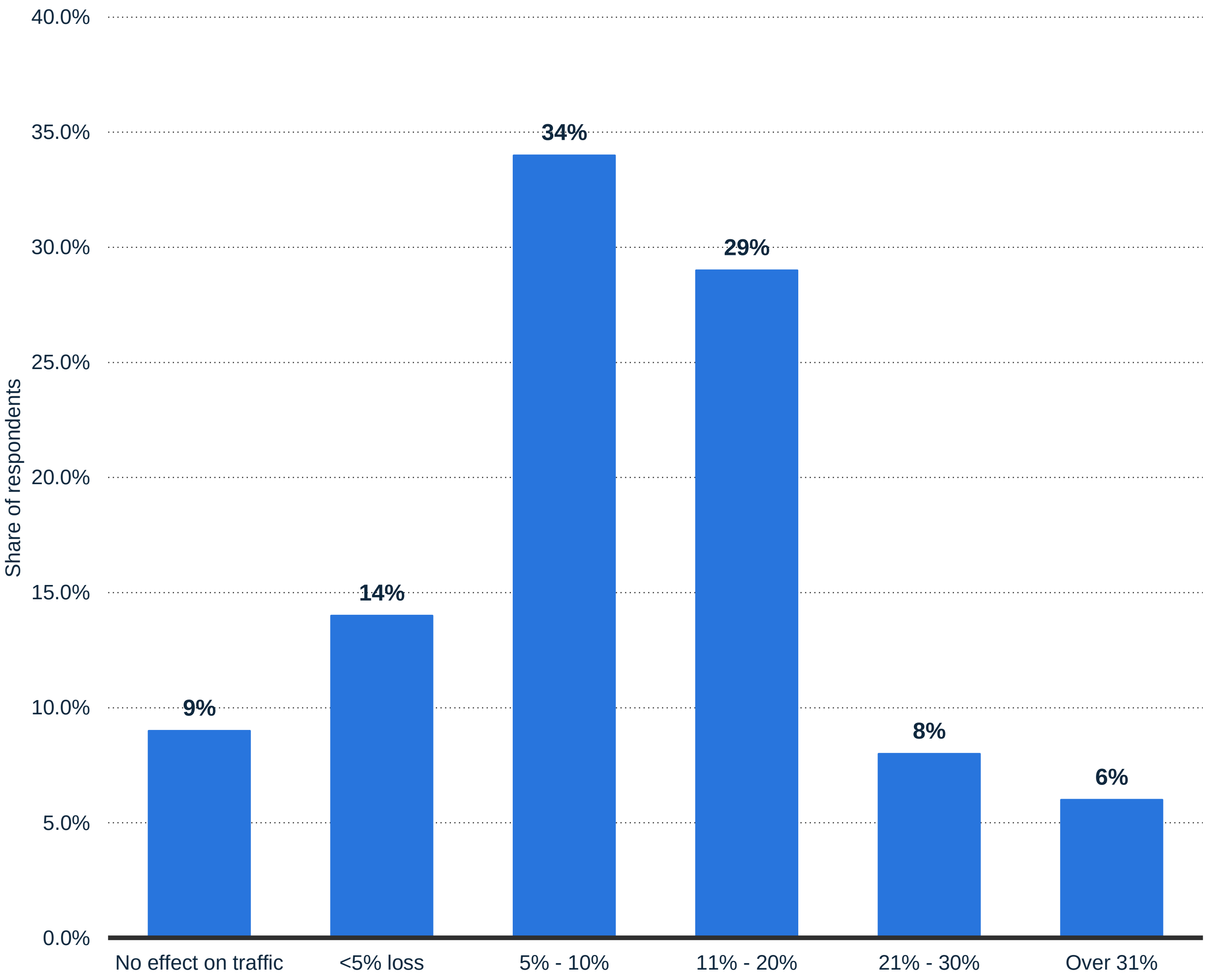
Digital ad spend in behavioral targeting in Europe in 2020, by scenario



What’s next?

Stricter rules on data privacy don’t end with the GDPR. By 2020, the ePrivacy Regulation might replace the existing ePrivacy Directive and set rules regarding data protection in electronic communications. The current draft will be applied in accordance to the GDPR principles and will contain further obligations with online data processing, especially regarding the use of cookies and online marketing technologies. Under the ePrivacy Regulation, website publishers will have to gain user consent before using cookie tracking for marketing purposes. Information on cookies will have to be clearer and not encourage users to consent too easily. Even analytics cookies provided by third parties like Google might require user approval. Less accurate cookie tracking results in less usable data on user online behavior. Therefore, investments in behavioral targeting for online marketing could be affected by data protection regulations. In a scenario of low impact, the value of investments in behavioral targeting is expected to be cut in half.

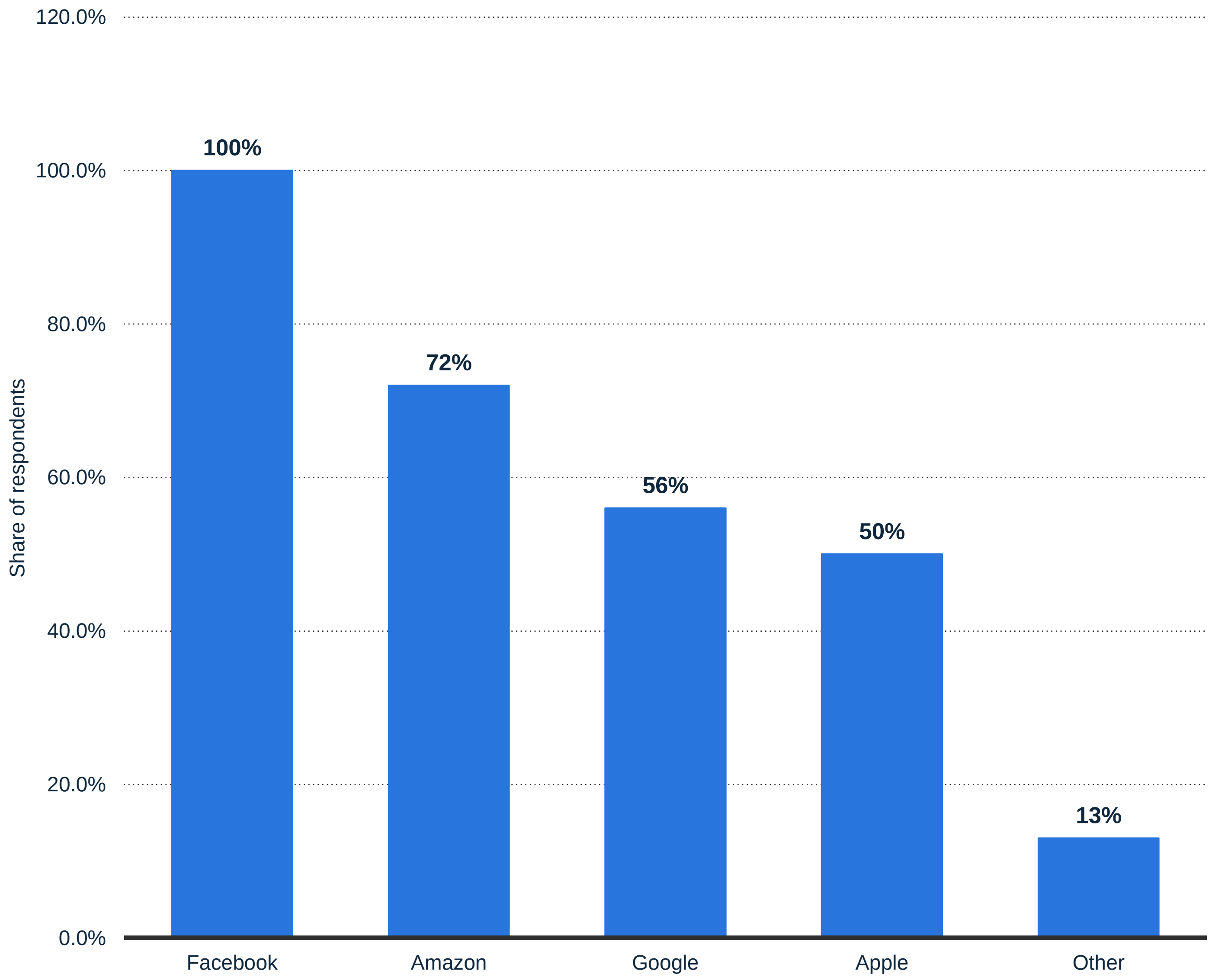
Note: Europe; 2017
Source(s): Statista



The next ePrivacy Regulation might cause web traffic loss

Under the ePrivacy Regulation, users will need to express clear consent to enabling cookies-before browsing a website. This could be set on browser level, similar to how current anti-tracking and ad-blocking software is operating. In general, cookie policies will be less ambiguous than they are at present. As a side effect, they would partially affect online traffic: In 2018, French and English marketers were asked how the next ePrivacy Regulation might affect the traffic of their websites. According to 34 percent of the surveyed marketers, websites might lose up to 10 percent of their traffic, while 11 percent of them estimated that the traffic would decrease by 20 to 29 percent. Less consent to cookie tracking for advertising might cause further losses in display advertising revenues. In Germany, VDZ, the national publishers' association, estimated that up to 300 million euros could be lost due to the ePrivacy Regulation.

Note: France, United Kingdom (Great Britain); 2018; marketers
Source(s): Mailjet



Who profits from ePrivacy according to German publishers?

The effectiveness of digital advertising depends on customer segmentation, but privacy regulations restrict the tracking of online behavioral data. Therefore, platforms where users are always logged in would obtain users' consent to data treatment more easily.

In a 2018 poll, all surveyed German publishers stated that Facebook would benefit from the ePrivacy Regulation due to the platform's massive login rates. Amazon followed with 72 percent.

Also, the survey showed that German publishers tend to provide content after the users' registration, as this would be the only way to obtain consent for data processing. In the future, users will need to subscribe for free content and publishers will need to invest resources in attracting users to the login step.

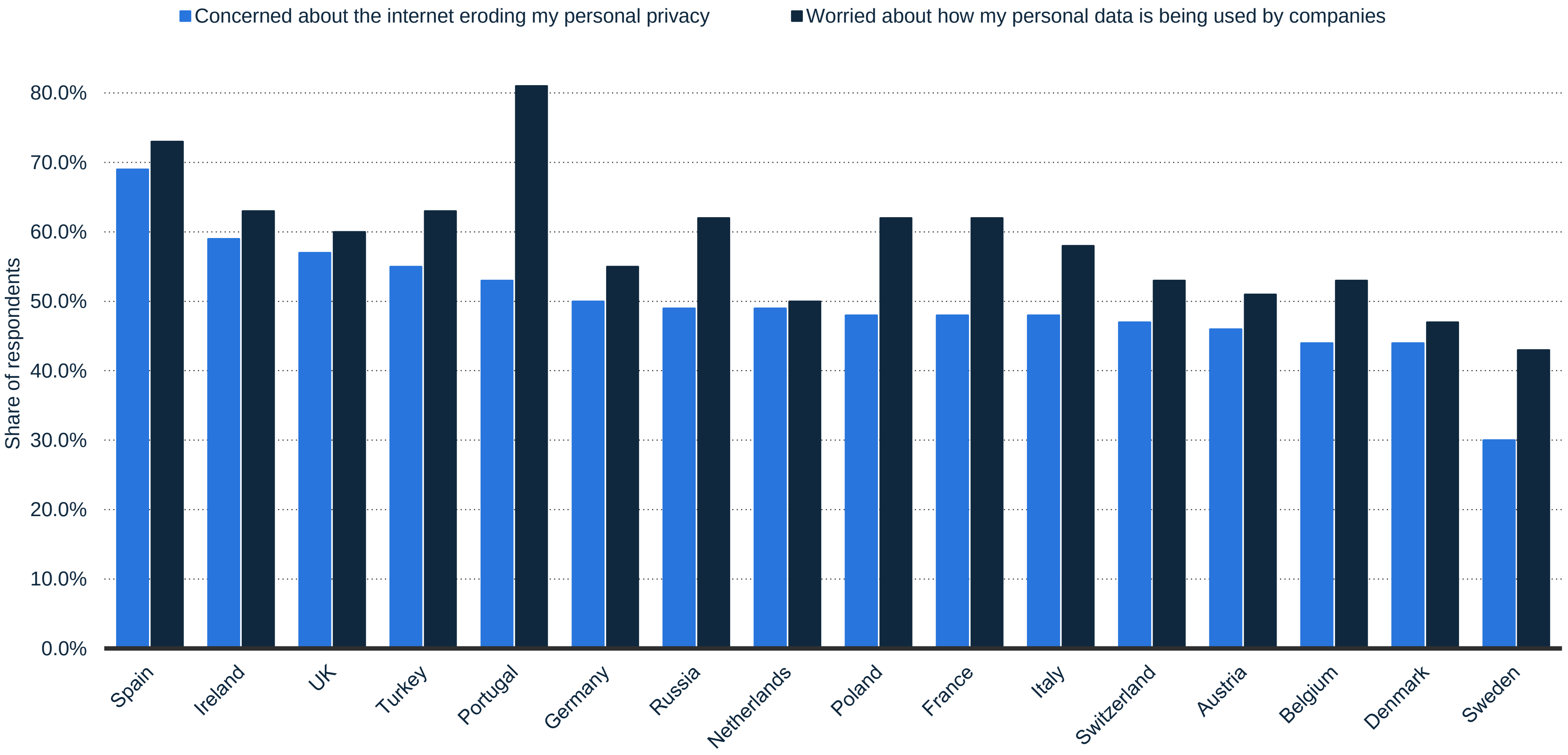
Note: Germany; 2018; Experts, CEOs of publishing groups who answered 'very strong'
Source(s): VDZ

05 **Privacy awareness**

- Trust in data processing
- User awareness of personal data

Internet users don’t trust companies using their data

Share of individuals concerned about use of personal data worldwide in 2018

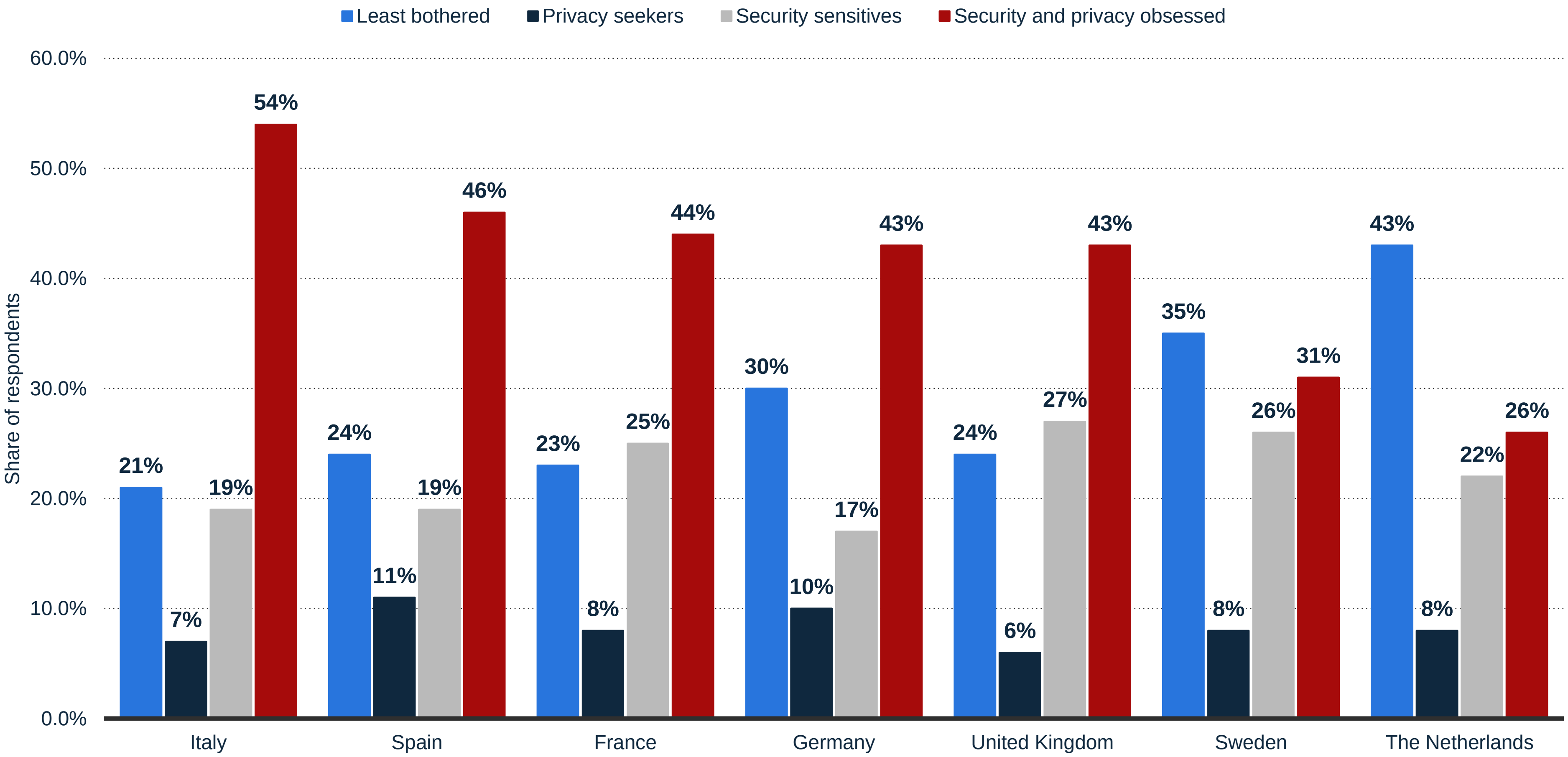


Despite the GDPR, large percentages of users are worried about the internet eroding their privacy. An even bigger share of individuals is worried that companies might misuse their personal data. Companies should build a trusted relationship with customers , especially in the area of online data management.

Note: Worldwide; April to June 2018
Source(s): GlobalWebIndex

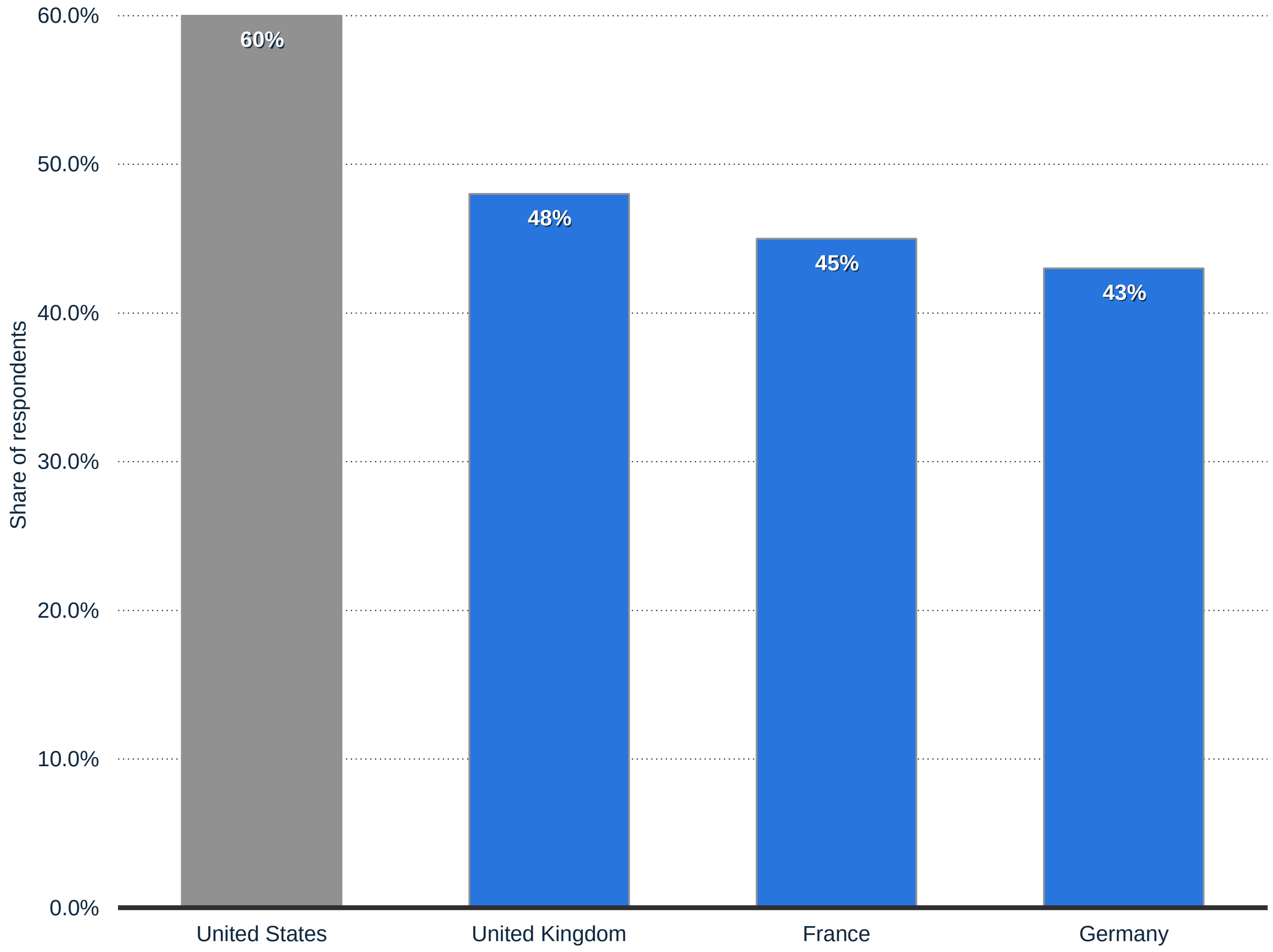
Consumers’ sensitivity to cybersecurity and data privacy in 2018

Share of consumers concerned about cybersecurity and data privacy in Europe in 2018, by country



A significant share of consumers surveyed by Capgemini defined themselves as ‘obsessed’ with data security and privacy. They considered the correct management of their data by retailers extremely important. However, they were willing to increase online spending if retailers assured safe data management.

Note: EU; January to February 2018; 18 years and older
Source(s): Capgemini



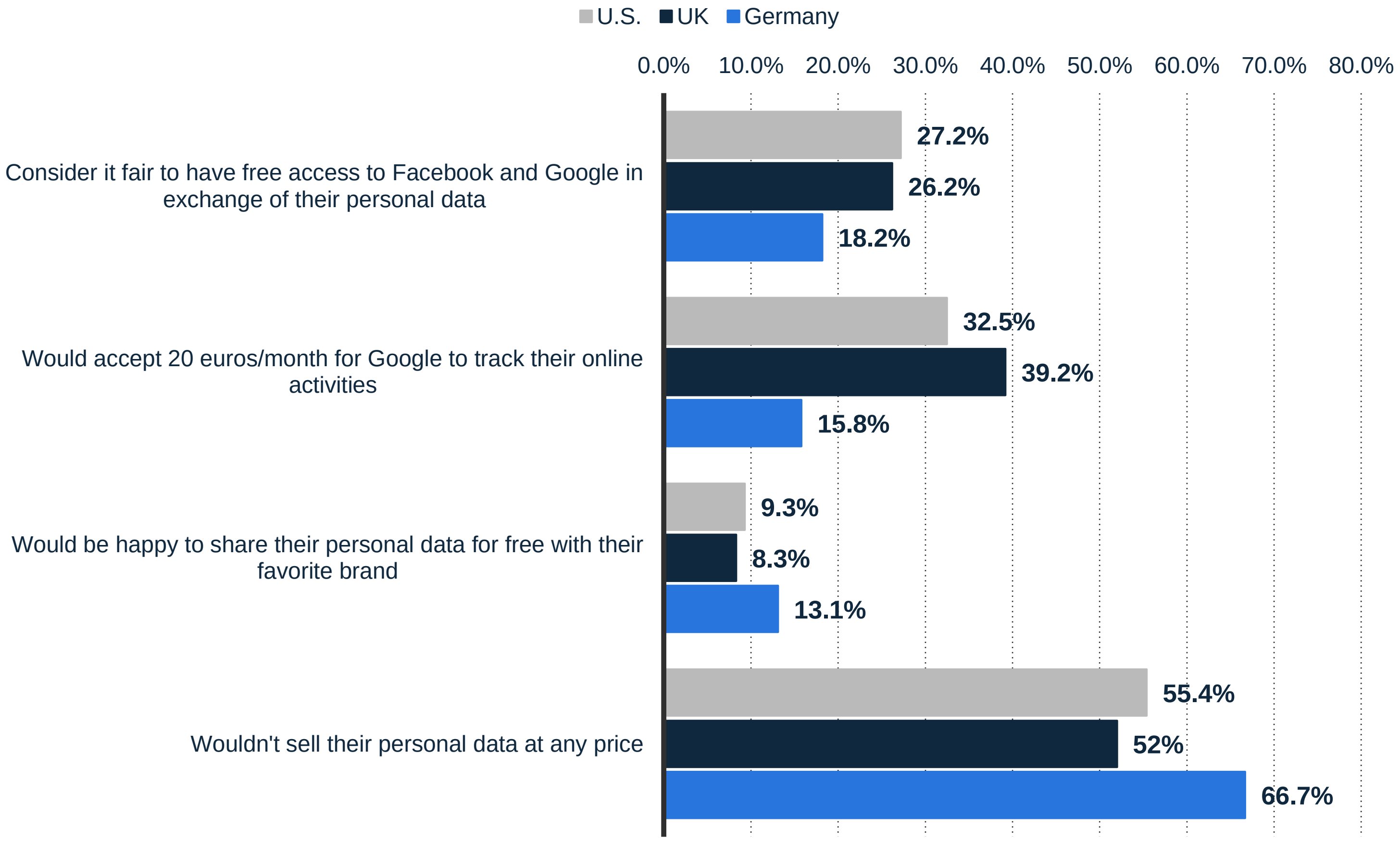
Consumers agreeing to ethical data use by companies in 2018

According to an RSA's study, 60 percent of U.S. consumers would agree to an ethical use of personal data by companies, and so would a lower percentage of European consumers. In any case, the conditions to share personal data would be two-fold: providing convenience and helping to protect. The first case implies the use of personal data as a commodity to be exchanged between companies. An example of the second condition could be the use of location data to track devices, or, for instance, to track payments and reject fraud transactions. The definition of "ethical use" is rather subjective across the countries depending on the type of tracked data.

Note: France, Germany, United Kingdom, United States; December 18-27, 2018; 18 years and older; 6,387 Respondents
Source(s): RSA

Personal data as a currency

Opinion on the use of personal data online in the EU and U.S. 2018



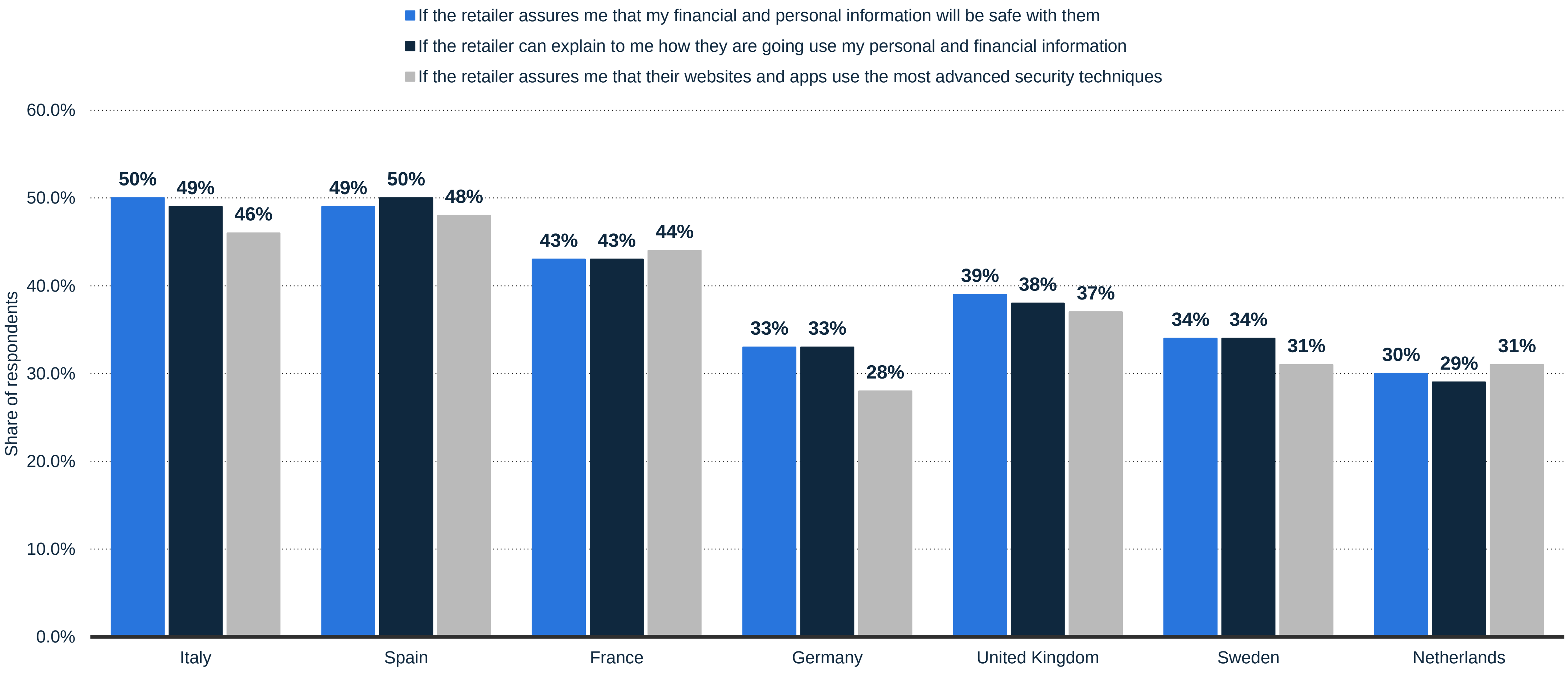
Data privacy trade-off

As mentioned before, personal data is an asset users might want to share under certain circumstances. For instance, about 40 percent of users answering a poll in the UK wouldn’t mind to be tracked online by Google for just twenty euros per month. The percentage of incorruptible users is higher in Europe than in the U.S. Additionally, 66.7 percent of users in Germany would not sell their personal information at any price, while only 52 percent of users in the UK have the same opinion. Data are being perceived as a medium of exchange with brands, and businesses will need to personalize deals for users to let them make compromises regarding their own privacy.

Note: Germany, United Kingdom, United States, EU; May 15-18, 2018; 18 years and older; 3,000 respondents; 1,000 respondents in each country
Source(s): Syzygy

Consumers would spend more online if their data were kept safely

Consumers' spending intentions with assurances regarding data safety 2018



Note: EU; January to February 2018; 18 years and older
Source(s): Capgemini

Key takeaways and upcoming trends

- **206 thousand cases of non-compliance and nearly 95 thousand data breaches have been reported since May 2018.**
- **EU companies invested more than U.S. ones in GDPR compliance.**
- **The GDPR is a complex regulation slowing down sales processes.**
- **Professionals responsible for data privacy will be more sought after on the job market.**
- **Third-party tracking placed by advertisers is limited, in favor of first-party tracking.**
- **Greater use of data encryption.**
- **Greater focus on safe data hosting.**
- **The next ePrivacy Regulation might bring less investments in programmatic marketing based on online customer behavior.**
- **The ePrivacy Regulation is expected to cause a drop in online web traffic and a loss in digital advertising revenues. Login procedures could be implemented for free editorial content.**
- **Despite the GDPR, users don’t trust companies processing their data, but would agree to sharing personal information in exchange for convenient products or services.**

Glossary

California Consumer Privacy Act – Legislation regarding data privacy for residents in California.

Consent management platform (CMP) – A set of rules presented to the users to gain their consent to data processing.

Data controller - (under the GDPR) Legal person, public authority, or agency that is responsible for data processing.

Data encryption - Technique replacing original data with a code which can be read only through a decryption key.

Data masking - Technique obscuring original data with different, not real data.

Data processor - (under the GDPR) Legal person, public authority, or agency that processes data on behalf of the data controller.

eCPM - Effective cost-per-mille, calculated as follows: cost per click * clicks / (impressions / 1,000).

ePrivacy Directive - It came into force in May 2011 and was expected to be replaced by the ePrivacy Regulation. It is about the processing of personal data and the protection of data privacy in the electronic communications sector.

First-party cookies - Tracking technology used by a website to track the visitors' movements.

OTT services – Digital providers of Over-the-Top content, e.g. OTT television.

Personal Information Security Specification – Legislation regarding use of personal data in China.

Privacy leader - Professional responsible for data privacy in a company, often an expert with legal experience.

Pseudonymization technique - Process where data cannot be attributed to an individual. Data masking and data encryption are techniques of pseudonymization.

Glossary

Retargeting – Online advertising cookie which tracks visitors of a website after they leave it.

Second-party cookies - Online cookies shared between two companies or websites under a partnership.

Third-party cookies - Tracking technologies issued by a domain while the user is visiting other websites. They are used for retargeting and displaying of advertising.

Sources

Capgemini
CDPInstitute.org
Cisco Systems
Cliqz
Data Protection Commission
Delphix
DLA Piper
European Parliament
Ernst & Young
GlobalWebIndex
International Association of Privacy Professionals
IBM
Kaspersky Lab
Mailjet
McDermott Will & Emery
Merril Corporation
PageFair
Reuters Institute
RSA
Smaato
Syzygy
Teads
TRUSTe
Uni Bochum
Verband Deutscher Zeitschriftenverleger
YouGov

Recommendations for further reading on Statista

DossierPlus

Cross-border e-commerce

Dossiers

Advertising & Privacy in the U.S. 2017

Online privacy

Online privacy and data protection in the European Union (EU)

Online privacy in the United Kingdom (UK)

Topic pages

Online privacy

Information security

DANIELA COPPOLA

Researcher – Internet, media, and advertising (Europe)

TEL	(040) 284 8410
E-MAIL	daniela.coppola@statista.com

WWW.STATISTA.COM