The state of adoption of Consumer Privacy in the US

Based on Europe's GDPR regulation

(January 2019)

A comprehensive market study testing the state of Consumer Privacy among 50 organisations in the United States, active in different verticals.

Introduction (1/2)

As of May 2018, the new privacy regulation General Data Protection Regulation (or GDPR) came into full force across Europe. Many organisations in Europe struggled to prepare in time; some were already fairly well-prepared, whilst others encountered major issues. There was a lot of speculation around GDPR and what would be needed to be ready for it. The regulation made it necessary for IT, marketing and legal departments within organisations to work closely together. Transparency had never really been the basis for interaction with consumers before, so marketing departments in particular had to completely adapt their vision, approach and execution. In the process, some organisations started to realise that GDPR was not only a limitation but rather a new way to build trusted relationships with their consumers and elevating their relationships with their users also giving them a competitive advantage. Today's consumers are increasingly aware of their privacy rights and more discerning about who to trust their personal information with.

In the run-up to GDPR, iWelcome commissioned a comprehensive research among 89 European organisations. After the first measurement in November 2017, our conclusion was that 89% of European organisations were not ready for GDPR. During the months that followed, we observed only minor changes but when the effective from date was announced a lot of companies adapted their policies. Especially in Northern Europe, companies shifted their attitude towards consumer data and privacy. GDPR signals the beginning of a new era with consumers being empowered with control of their own data.

Other privacy acts

It is in our nature to be curious: After the great success of our European research, we were interested to see if other parts of the world are following suit and becoming more privacy-savvy as well. Organisations across the world doing business with European citizens are also bound to comply with the legislation, which automatically means GDPR is not solely a European affair. On top of that, similar legislations are being designed, for example the California Consumer Privacy Act. With this regulation being introduced last June, we decided to put American companies to the test.

How do they perform when it comes to Consumer Privacy?

Our US research

iWelcome performed an assessment on Consumer Privacy awareness, testing 50 US organisations across different verticals. The verticals analysed are:

- Insurance;
- Utilities;
- Media & Publishing;
- Travel & Services;
- Retail/E-tail & Consumer Products.;
- Non-Profit.

Introduction (2/2)

Although the California Consumer Privacy Act and GDPR are different legislations, their approach towards Consumer Rights is quite similar. As such, we took GDPR allowing us to better compare results with Europe. As these regulations in essence are meant to help customers; we investigated the state of compliance from a consumer's perspective.
We assessed the customer registration processes and privacy statements of organisations and compared the current state to how it should be implemented under the GDPR.

Following this approach, we were able to measure the following GDPR variables:

- Consent (GDPR article 6 and 7);
- Ability to withdraw (GDPR article 7);
- Right of access (GDPR article 15);
- Right of rectification (GDPR article 16);
- Right to erasure (GDPR article 17);
- Data retention period (GDPR article 5.1(e));
- Privacy by default (GDPR article 25);
- Special categories of data, when applicable (GDPR article 9).

Parental consent and data portability are also relevant from a consumer's perspective, but due to the research methodology, we weren't able to measure these variables.

GDPR as a business enabler

In our view, the goal of the new privacy regulations is to protect customer data held by companies and organisations. In practice, this means that individuals are being put back in control of their own data. If data controllers don't comply with the regulation, they risk hefty fines and risk to their brand. However, we strongly believe that compliance should not be the sole motivation to adhere. GDPR should be a mindset, embedded in an organisation's DNA, as a new way to interact with consumers and build trusted relationships with them. Therefore, the goal of this research is to raise awareness among organisations worldwide regarding new ways to build trusted relationships with customers and to support organisations on their journey to compliance.

If you want to know how compliant your organisation is when it comes to customer interaction under GDPR, you're invited to take our online self-test.

Overall results (1/2)

Overall, we see that only 16% of all organisations from the sample are starting to fulfill most GDPR-requirements or are almost to fully compliant. This means a staggering 84% of US companies are nowhere near being compliant.
The average GDPR-compliance score is 4.87 out of 10. This shows that American companies in general have not really adopted a GDPR state of mind yet. Moreover, it seems that also the new California Consumer Privacy Act has not materially influenced behaviour towards consumers as yet.

We analysed different GDPR-requirements that will be explained in the following chapters. In addition, we found some additional interesting results:

- Firms included in the research that reside in California score higher than firms located in other states;
- Firms with an office or subsidiary in the EU scored relatively better.

- A staggering **84%** are nowhere near being compliant;
- Firms included in the research that reside in **California** score higher than firms located in other states;
- Firms with an office or subsidiary in the **EU** scored relatively better;
- Some firms offer certain rights exclusively for California residents.

Exclusive rights for Californians

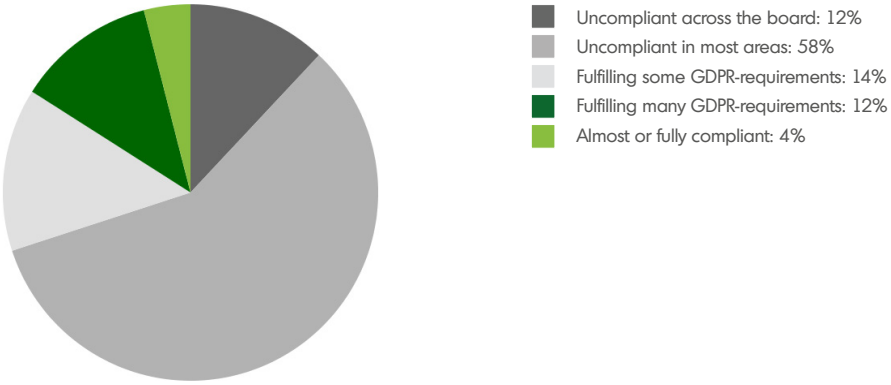
Some firms offer certain rights exclusively for California residents. In multiple privacy statements we encountered that the right of access to personal data was solely offered to Californian customers. This is quite remarkable, because it means that processes are already in place to support the directive. So why not offer the right of access as a service to all customers? This observation illustrates that the approach towards regulations is often driven from a compliancy perspective. As we advocate; privacy laws should be a co-operation between marketing, IT and legal departments to initiate a new and future-proof approach towards the customer.

Results: USA vs. Europe

We do believe that with the GDPR, a standard has been set that eventually will be followed by other countries. In June we performed our fifth measurement in Europe. We have used those results to compare the current state of GDPR adoption in the USA to Europe.

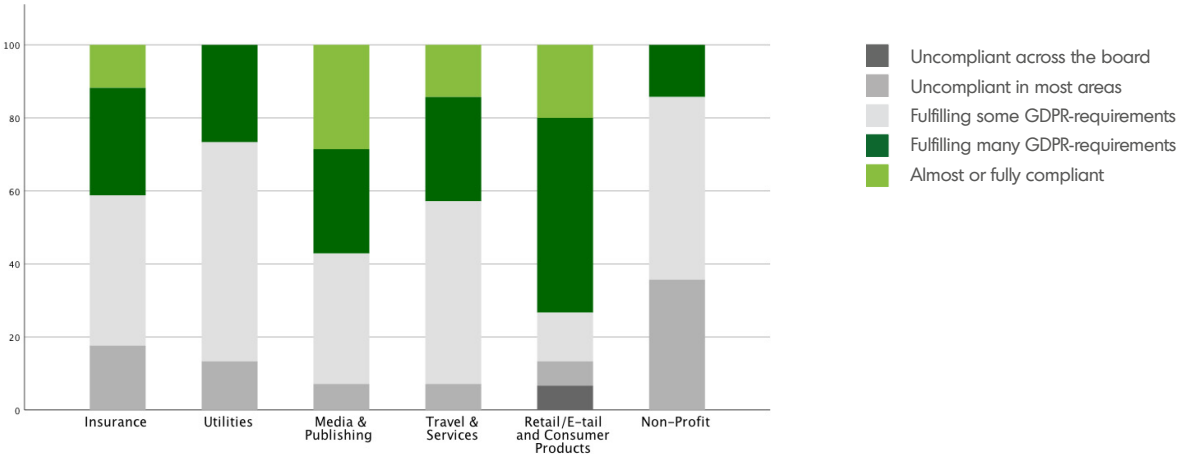
It is clear that the USA are still far behind, especially compared to Northern European countries, but we also see companies that are doing a better job and are creating new market standards. In Switzerland, Spain and France we did not observe any firms that are almost to fully compliant. In the USA we did spot a few, all are organisations that operate across borders.

Overall GDPR-compliance



Overall results (2/2)

Overall compliance. USA compared to Europe.



Average scores per country

Country	GDPR-compliance average score
United Kingdom	8.24
Germany	8.16
Sweden	7.80
Netherlands	6.90
France	6.85
Spain	6.29
Switzerland	5.69
USA	**4.87**

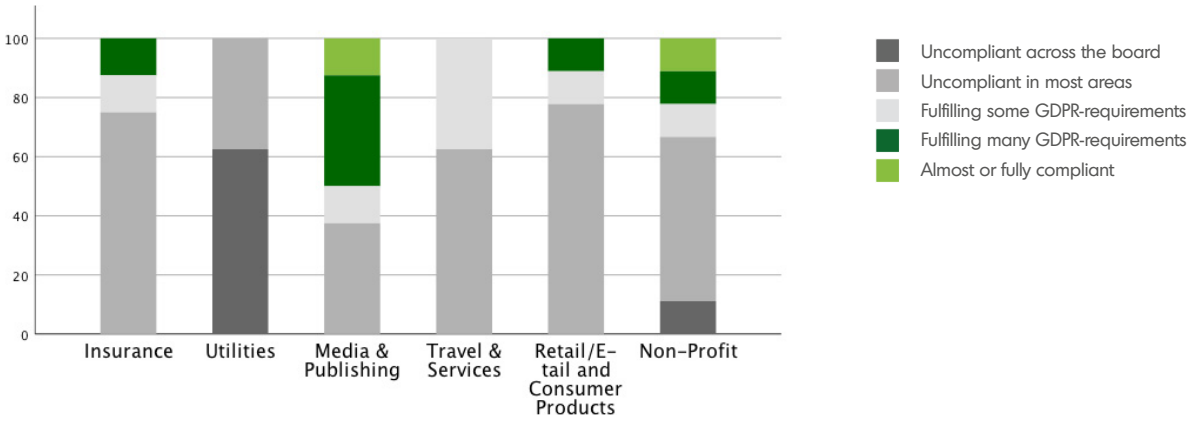
Results on an industry-level

Overall, there is significant variation between different industry verticals. In the figures, you'll see an average score and a graph that shows how the different companies within the vertical score. We see that Utilities for example, has the lowest score and in the graph, you'll see that this is reflected across the assessed organisations. They all are positioned in 'Uncompliant across the board' and 'Uncompliant in most areas'. Media and Publishing scores highest. This is partly thanks to a few very high performing organisations whilst other parts of the Media industry lag behind.

Some of these differences can be explained based on customer population. According to GDPR, US companies that do business with European citizens should be compliant to the regulation. Insurance and utilities are more likely to sell their products in a home market, which explains that they stay behind.

- **Media & Publishing** scores best with an average of 6.20 out of 10;
- **Utilities** scores lowest.

GDPR score specified per industry



Average scores per industry

Industry	GDPR-compliance average score
Media & Publishing	6.20
Travel & Services	5.56
Insurance	5.11
Retail/E-tail & Consumer Products	4.98
Non-profit	4.96
Utilities	2.38

Consent (1/2)

One of the most important aspects of the GDPR is "Consent". If the processing of data is not covered by one of the bases for processing as stated in the GDPR (e.g. the performance of a contract), a consumer needs to give consent for the use of his or her personal data. The use of the data should be linked to one or more specific purposes, that need to be specified per attribute.

In our research, the element of consent was measured by looking at the following aspects:

- Is consent being asked for in a straightforward manner? For example, can the consumer tick a box to grant permission for their data to be processed?
- Is the purpose of use mentioned at all? Does the organisation clarify for what purpose the personal data will be used?
- Is the purpose of use crystal clear?
- Is the purpose of use specified per attribute?

- **Media & Publishing**, **Retail/E-tail** and **Consumer Products** score highest;
- 86% of **US organisations** hardly implemented consent.

Purely looking at the consent-sphere, the results of our analysis show that most of the American firms are fulfilling 'some' GDPR-requirements. The average score is 1.88 out of 4.

In an ideal situation of a consumer registering with an organisation, an organisation should **request** consent for the use of certain personal data **and** provide a purpose of use per attribute. In the sample, we've observed that consent is often being asked by means of agreeing with a privacy statement instead of asking for consent in a straightforward way. The purpose of use is often not clear at all. Especially in situations where processing of data for marketing purposes is the case; this is often either vaguely described or mentioned in a privacy statement, without requesting straightforward consent. On top of that, the data controllers in the sample often lack a clear link to the privacy statement; in many cases you would need to search for it on the website which is clearly not compliant.

Consent score per industry

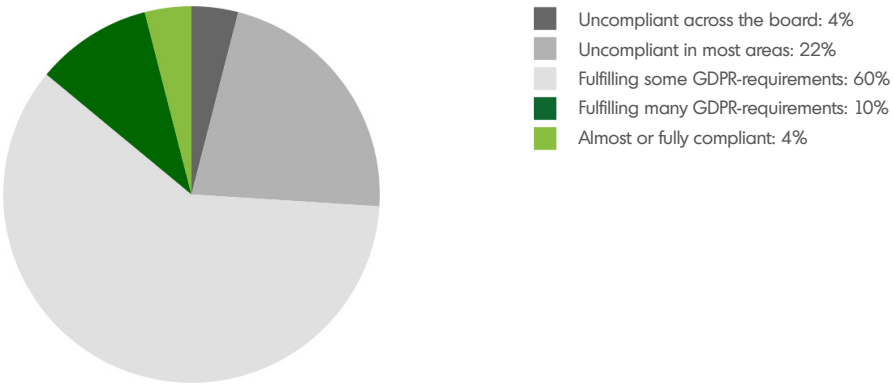
The graph illustrates that Media & Publishing and Retail/E-tail and Consumer Products are scoring relatively well on consent; some of the data controllers are fulfilling many GDPR-requirements or are almost or fully compliant.
This has also been the case in our European research and is no surprise, since these verticals are known to be digital frontrunners with high online competition. Utilities is the vertical that scores lowest, but there is an important point to note here: Some of the companies indeed lack the question for consent when needed but in some cases utility companies only ask a few personal details needed to perform a contract and it is hard to judge whether consent should have been requested or not.

Consent score compared to Europe

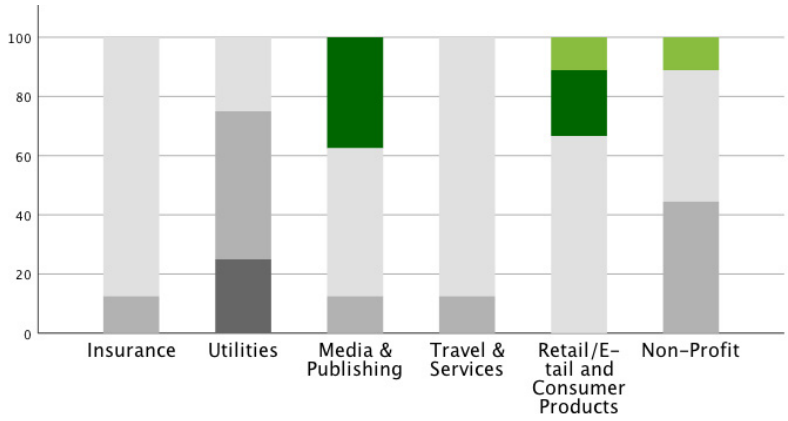
In comparison to Europe, the USA score poorer on the consent aspect. Most of the sample is positioned in the categories 'Uncompliant across the board', 'Uncompliant in most areas' and 'Fulfilling some GDPR-requirements'.
In Europe, 42,7% of data controllers as a whole are 'Fulfilling many GDPR-requirements' or 'Almost or fully compliant', with the UK and Germany being frontrunners. This percentage is only 14% for the USA.

Consent (2/2)

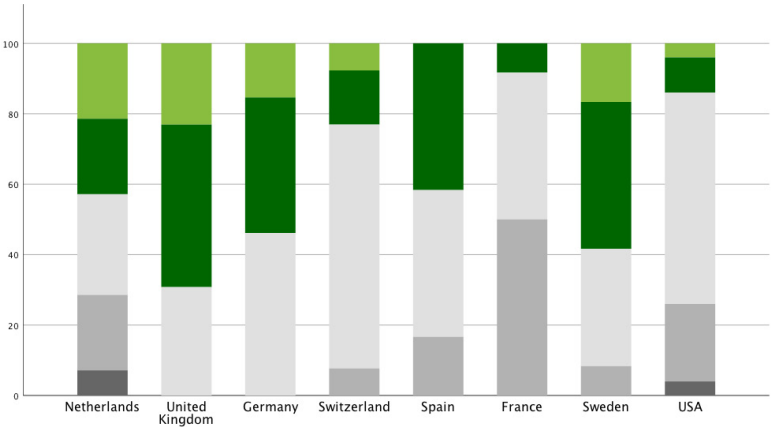
Overall score on consent



Consent score per industry



Consent score USA compared to Europe



Ability to withdraw

Consent must be given freely; specificly, informed and unambiguously. An individual must have the possibility to withdraw their consent at any time, just as easy as it was given.

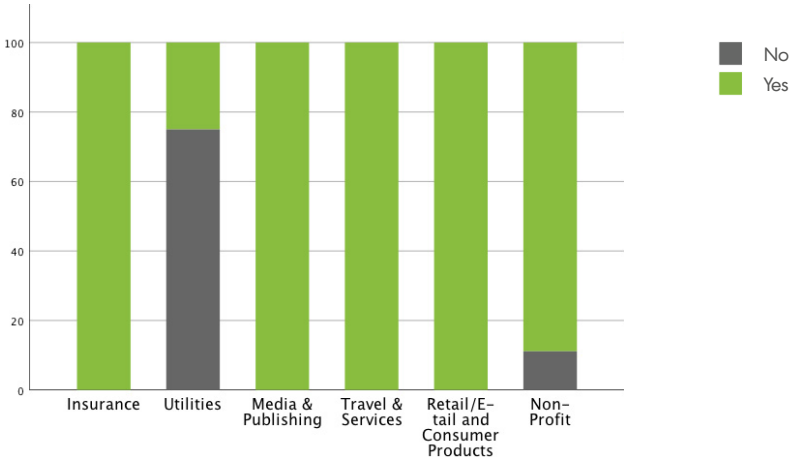
- Does the data controller make the individual aware of the fact that consent can be revoked?

- **14%** does not address the ability to withdraw consent;
- Organisations that do mention the ability don't have a fine-grained mechanism for this.

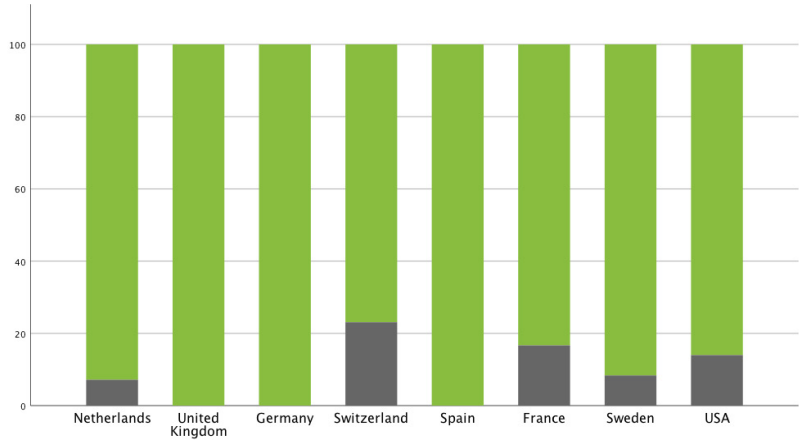
As the right to withdraw is not always visibly presented in the registration process, we also investigated the privacy statements and the procedure for revoking consent for receiving newsletters. In 14% of cases the ability to withdraw is not addressed in the registration phase, nor in the privacy statement. In 86% of cases there is a mention of revoking consent, most of the time for newsletters and marketing subscriptions. The extensiveness and ease of use however, is not satisfactory. Ideally it should be possible to easily revoke consent per data attribute/field.

On a European level, the percentage of companies that do not address the right to withdraw at all is 7.9%. The laggards are Switzerland (no GDPR, but similar legislation) and France. On a country level the USA score better than either of these two.

Ability to withdraw. Score per industry.



Ability to withdraw. USA compared to Europe.



Right of access (1/2)

Under GDPR, European citizens have the right to obtain information on whether or not their personal data are being processed. If that is the case, there is a right of access to that data (including amongst others the purpose of use and the envisaged period for which the personal data will be stored). Moreover, this right should be free of charge. The California Consumer Privacy Act offers a similar right of access.

- Is the right of access mentioned? Can this right be exercised free of charge?

In our American sample, 36% of firms do not offer the right of access at all. For Europe, this percentage is only 3.4% (and these are all Swiss organisations). In the USA there are no observations where an administrative fee for an overview of processed personal data is required. The right is either offered for free (but limited to a reasonable amount, e.g. once a year) or not offered at all. Utilities score badly and do not provide the right of access at all, closely followed by the insurance sector.

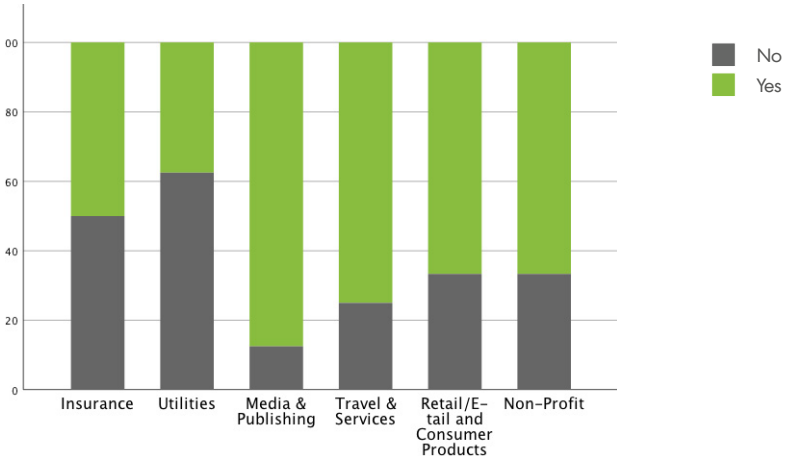
- **36%** of firms do not offer the right of access at all;
- In Europe this is **3.4%**;
- Remarkably, multiple firms only offer the right of access for California residents.

Exclusively for California residents

We have to add a critical note here: multiple organisations that grant the right of access specify that it is exclusively available for California residents. This shows that for most companies privacy and trust are not yet a state of mind or a service towards a consumer, but purely a compliancy-issue. In our view this is a missed opportunity for a better engagement with all customers especially considering that the processes designed to enable the right of access (in these cases) are in place. In Europe organisations are starting to see the advantage of privacy and its role in building trusted relationships with customers. We do not really sense this in the USA as yet.

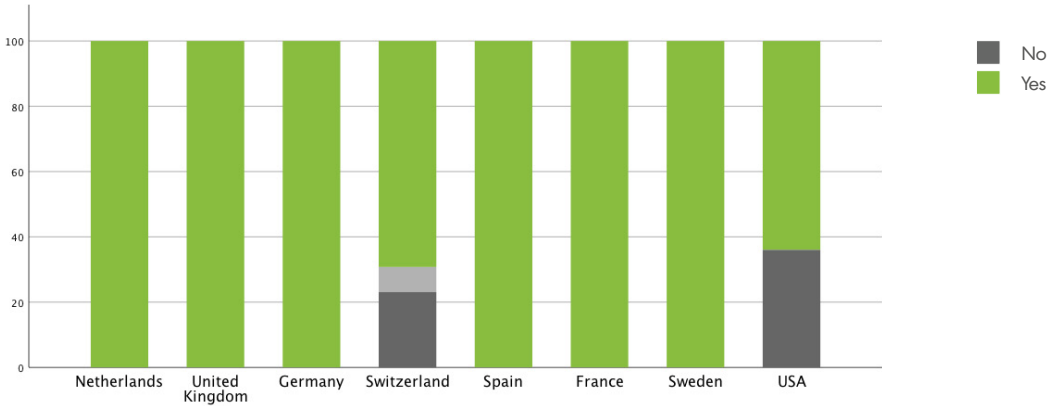
With regard to the difference between the USA and Europe: In the European market, the intoduction of GDPR in May 2018 kickstarted and drove change with the regulation anticipated in the preceding months and even years. In our first edition of the European research (November 2017) the situation was more akin to the first instalment of the American research. Back then the European percentage for not providing the right of access was 34%. This shows that huge leaps, in a relatively short space of time, can be made if organisations are willing to become more customer-privacy focussed and their awareness raises.

Right of acces. Score per industry.



Right of access (2/2)

Right of acces. USA compared to Europe.



Right of rectification

Under GDPR, consumers have a right to rectification of their data when incorrect or incomplete. Data controllers must point out this right in a clear and concise manner.

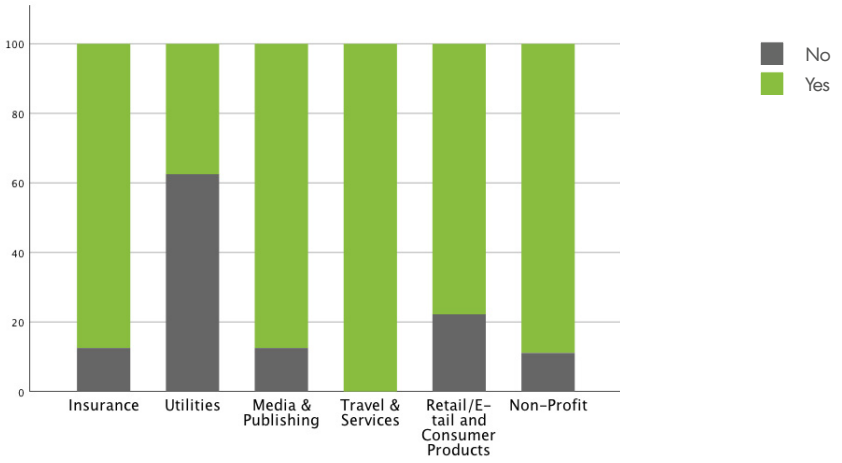
- Is the possibility for rectification mentioned anywhere?

The right of rectification is not offered in 20% of cases. For Europe as a whole, this percentage is only 4.5% (and these are all Swiss, so all other countries score 100%). Worth mentioning is that our whole sample in Travel & Services does offer this right.

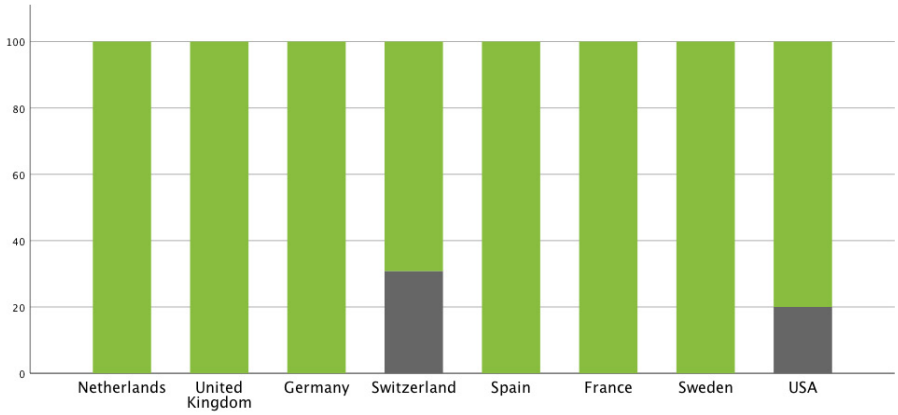
Again, only in Switzerland observations occurred where firms did not provide the right of rectification in industries 'Insurance' and 'Utilities'.

- **20%** of firms do not mention the right of rectification at all;
- **Travel & Services** scores best.

Right of rectification. Score per industry.



Right of rectification. USA compared to Europe.



Right to erasure

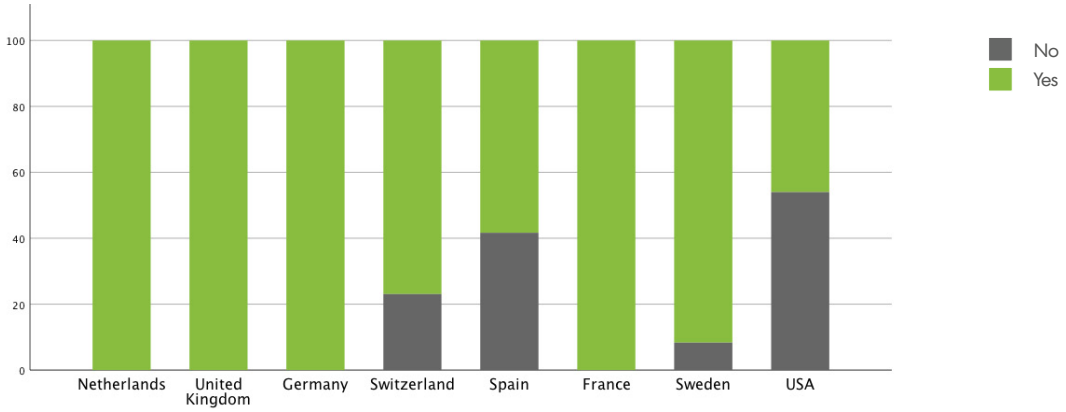
Initially known as the right to be forgotten, the right to erasure empowers consumers to demand erasure of their personal data, unless processing is necessary for specific reasons stated in the regulation, such as compliance with law. In all other case, it must be possible for consumers to completely have (all) personal data held by organisations.

- Is the right to erasure mentioned?

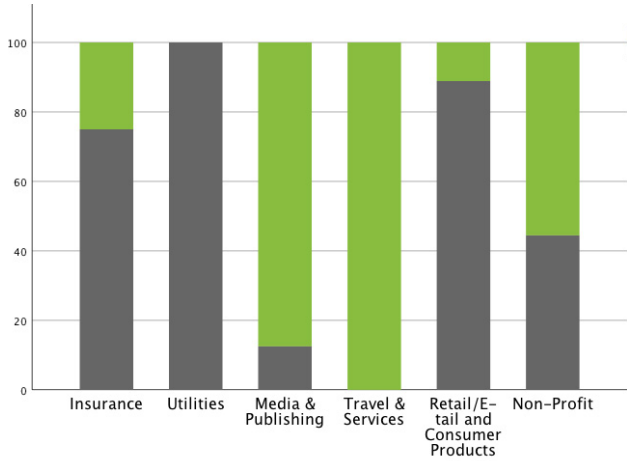
In our American sample, the right to erasure is not offered in 54% of cases. Quite a large percentage compared to Europe's percentage of 10%.
In the Utilities sector, no single firm offers this right. Other sectors performing poorly on this aspect were Insurance and Retail/E-tail and consumer products. The entire Travel & Services sector does consistently provide this right.

- **54%** of firms do not mention the right of rectification at all;
- A huge gap with Europe, where **10%** fails to offer this right;
- **Travel & Services** scores best.

Right to erasure. Score per industry.



Right to erasure. USA compared to Europe.



Data retention period

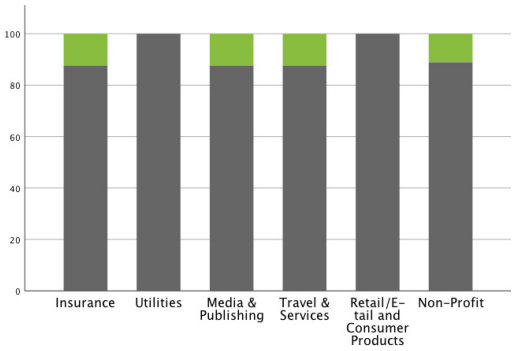
Data controllers need to be transparent about the period for which data will be stored. This period can be subject to external circumstances, such as legal obligations or research purposes. The data retention period should be specified, per category of data. After this period, data should be deleted.

- Is the period for which consumer's data will be stored specified?

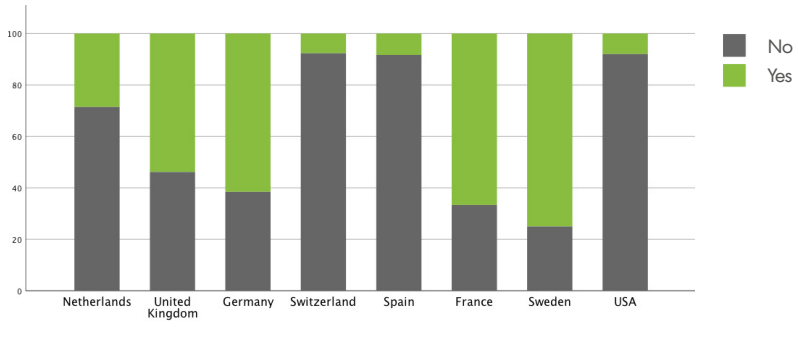
A stunning 92% of American data controllers do not specify the data retention period. European data controllers are also underperforming on this aspect of GDPR. Sweden is relatively seen the best scoring country and the USA by far the worst. The issue is the specification of the data retention period. Often, American firms do have a data retention policy, also referred to in their privacy statements but the exact period is not specified or too vague. "We keep your data as long as needed to fulfil the purpose it was collected for" is often used to cover it. However, it should be more exact and specified per type of data (e.g. 36 months after your last purchase). The Utilities and Retail/E-tail & Consumer Products sectors all did not specify the data retention periods.

- **92%** of American organisations do not specify the data retention period;
- Data retention policies are refered to, but they are not specified;
- **Utilities** and **Retail/E-tail & Consumer Products** score lowest.

Is the data retention period specified? Score per industry.



Is the data retention period specified? USA compared to Europe.



Example of a specified data retention period:

What is the legal ground to process your personal data?
The processing of your personal data is necessary for H&M to fulfil the service of managing and delivering the order to you.

How long do we save your data?
We will keep your data as long as you are an active customer.

For customers with an account or Club membership we will keep your personal data for 36 months after your last purchase.

For customers with a guest checkout we will keep your personal data for 6 months after your last purchase.

Automated decision making:
When you apply for credit as a method of payment we will perform an automated decision-making process regarding your credit application. You have the right to to express your point of view and to contest the decision with a member of staff.

Privacy by default

An organisation's online environment should be designed in such a way that privacy is always the basis and consumers are in control. Consumers should not automatically receive information they did not ask for. There has to be an active opt-in. This also means that a pre-ticked box to receive a newsletter is not according to privacy by default and will no longer be sufficient under GDPR.

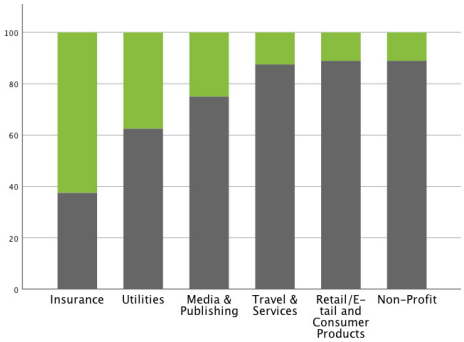
- Are there any 'pre-ticked boxes'? Can the consumer make his/her own decisions while interacting with the organisation online?

72% of American organisations have not designed their online customer environment according to the principle of privacy by default. Compared to Europe where 39.3% have not. The Insurance sector is performing best on this aspect, having no pre-ticked boxes in their registration procedures or making decisions without an opt-in from the customer. The Retail/E-tail & Consumer Products and Non-Profit sector are scoring relatively lowest on this aspect. For Non-Profit this might be explained by the observation that organisations often automatically send their donators a newsletter, assuming they would want to receive it. Under GDPR this approach would not be permissable.

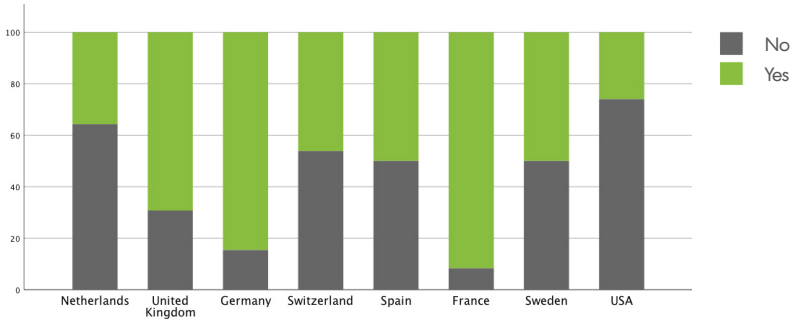
- **72%** of American organisations do not act according to privacy by default;
- In Europe this is **39%**;
- **Insurance** scores the best across the verticals assessed.

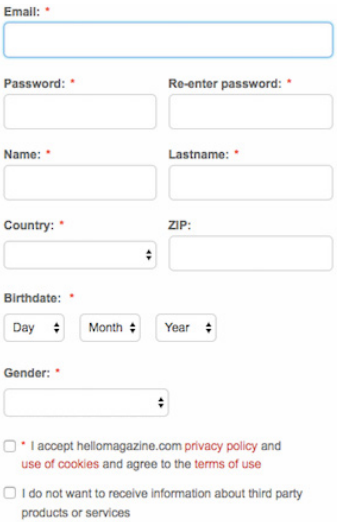
In general, we see that the mindset around opting in and receiving unsolicited marketing communications is quite different to Europe. Vague statements as "If you tell us you don't want to receive marketing messages we will stop sending them" are often encountered. In Europe an active opt-in should be given whereas in the USA the default settings seem to be dictated by marketing departments. The California Consumer Privacy Act differs at this point from GDPR and advocates an easy opt-out of selling personal data to third parties.

Privacy by default. Score per vertical.



Privacy by default. USA compared to Europe.





<<< Example of how not to act: newsletters will be sent unless a consumer opts out

Special categories of data

The GDPR specifies 'sensitive personal data' as special categories of personal data. In order to process this type of data, organisations must ask consumers for explicit consent with only a subtle difference compared to 'regular' consent. 'Regular' consent can be obtained by an affirmative act (for example: "by providing your email address, you agree to.."), but 'explicit' consent means that an individual must take affirmative action such as ticking a box to agree to the use of his or her sensitive data.

- Racial or Ethnic Origin
- Political Opinions
- Religious or Philosophical Beliefs
- Trade Union Membership
- Health
- Sex Life or Sexual Orientation
- Genetic or Biometric Data

- Does the organisation ask for explicit consent when making use of sensitive data?

Not all organisations in our research process special categories of data. This is why we only measured this variable for a limited number of industries, such as insurances (we tested travel insurances where health information is often asked for) and travel (e.g. diet information passed along to a travel organisation may reveal information about an individual's health or religion). The results show that 22.2% of American firms that process sensitive data, are actually processing these data with the explicit consent of the data prospect, therefore being compliant to the GDPR. This means that 77.8% of US firms don't comply to the GDPR when it comes to sensitive data. In Europe it's slightly better, a small majority of 52% of the data controllers collecting sensitive data process them only with the explicit consent of the customer.

The first one is a streaming video service, so why do they even have access to sensitive data?

"For example, we take steps to limit access to sensitive information from or about you to those employees, agents, and contractors who have a legitimate business reason to access such information. We also use measures like encryption and hashing to help protect sensitive information when in transmission."

Another data controller specifically mentioned that they do not want to receive any sensitive data from their customers.

Conclusions & What's next?

In general, we see that US organisations lag rather far behind when it comes to maintaining Consumer Privacy, with 86% being far from GDPR compliance. Our finding is that the overall mindset towards privacy seems to be different as from Europe, also being illustrated by the differences in the GDPR and the California Consumer Privacy Act. Still, US organisations that interact with Californian citizens need to comply to California law and organisations that interact with European citizens need to comply to GDPR, so many American organisations will need to implement changes.

Moreover: valuing consumer privacy should not strictly be about compliance. In a world where consumers are more and more privacy aware, and where the ambition for the California Consumer Privacy Act started as a ballot initiative, companies need to go back to the very core of doing business: put back focus on the relationships with their customers.

The question that arises therefore is: will organisations go for short-term marketing gain with the risk of reputation damage and fines, or do they build long-term trusted relationships based on transparency and consented use of personal data?

This creates an opportunity for the frontrunners to outsmart competition by investing in empowering customers with full control over their personal data. This 'next-level' mode of interacting with your customers demands a fair amount from an organisation's IT data infrastructure. According to Gartner , Consumer Identity and Access Management (or: Consumer IAM) is a core discipline to support digital business initiatives and strategic change.

Recognised as product and innovation leader with fine-grained GDPR support in Consumer IAM, iWelcome can support these frontrunners.

"iWelcome provides unparalleled consent management features."
KuppingerCole

"iWelcome offers EXCELLENT support for B2C use cases and for European GDPR compliance"
2016 Gartner Critical Capabilities for IDaaS, Worldwide

About iWelcome

iWelcome provides Identity as-a-Service for frictionless privacy-protected consumer services and security-enabled workforce processes. iWelcome is the only European born Identity Platform – headquartered in Europe, backed by European investors and specifically serving customers doing business in Europe. Millions of consumers and hundreds of thousands of employees - across industries like banking, insurance, utility, media & publishing, travel & services, retail/e-tail and Governments & Non-Profit – rely on iWelcome on a daily basis. Analysts like Gartner and KuppingerCole have recognised iWelcome as a worldwide Product and Innovation Leader with "Excellence" ratings.

Building truly winning partnerships with its customers, iWelcome offers lowest Total Cost of Ownership and a time-to-service in weeks. Applying Best-of-Breed Private Cloud Technology, customers benefit from both ends: using a SaaS service while not having to share critical resources.

+31 33 445 05 50 I info@iwelcome.com I www.iwelcome.com