welcome
europe's identity platform

The state of GDPR-readiness in Europe

A consumer perspective

(5th Edition: July 2018)

A comprehensive market study testing the state of GDPR readiness among 89 organisations from seven countries active in different verticals

Management Summary (1/2)

The moment we've all been waiting for has finally arrived: GDPR has come into full force in Europe. Many organisations in Europe struggled to get ready; some were already well-prepared while others encountered major issues. During the last eight months iWelcome has monitored European organisations on their GDPR readiness through the eyes of the consumer. The findings were published every two months.

After the first measurement in November our conclusion was that 89% of European organisations was not ready for GDPR. During the months to follow we saw minor changes in the measurement rounds. There was some improvement, but only in small elements. No significant changes were made, and it was most certainly not enough to be compliant. Even in April and May 2018, with the date approaching, we still noticed a lot of non-compliant issues in our research and overall only small improvements were measured.

Before you lies the fifth edition of our research, reporting on our measurement in June 2018 (after GDPR). The results are very interesting. There has been a clear shift. Where in the months before GDPR only small changes were measured, we now observed major changes. Data retention policies where introduced, companies introduced completely new privacy policies, etc.

Some of the most important findings:

- 33.7% is uncompliant in most areas or is only fulfilling some GDPR-requirements (compared to 66.3% in early May);
- 66.3% of the sample is fulfilling many GDPR-requirements or almost or fully compliant (compared to 33.7% in early May);
- The United Kingdom is the winner with an average score of 8.24, followed by Germany with a score of 8.16 and Sweden with 7.80 (out of 10);
- The winning vertical is Retail/E-tail & Consumer Products with a score of 8 out of 10;
- None of the organisations in our sample scores 'uncompliant across the board' anymore.

- **33.7%** is still uncompliant in most areas (compared to **66.3%** in early May);
- Out of 7 countries, The **United Kingdom** scores highest;
- The winning vertical is **Retail/E-tail & Consumer Products**;
- None of the organisations score 'uncompliant across the board' anymore.

Our research

iWelcome has been putting organisations throughout Europe to the test, performing a bi-monthly assessment on GDPR-compliance on customer interactions for 89 organisations across 7 countries: the Netherlands, the United Kingdom, Germany, France, Switzerland, Spain and Sweden. The verticals in scope are Insurance, Utilities, Media & Publishing, Travel & Services, Retail/E-tail & Consumer Products and Non-Profit.

GDPR as a business enabler

The goal of the regulation 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 fines. However, we strongly believe that this should not be the motivation to be compliant. GDPR should be a mindset, embedded in an organisation's DNA, as a new way to interact with consumers and build trusted relationships.

Management Summary (2/2)

As GDPR in essence is meant to help customers, we decided that the strongest approach is to investigate the current 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.

As mentioned earlier, the assessment is performed every two months. This is the fifth edition, reporting on the fifth measurement in June 2018. The first edition was published in December 2017 (measurement October and November 2017), the second one in February 2018 (measurement December 2017 and January 2018), the third one in April 2018 (measurement February and March 2018) and the fourth one in June (measurement April and early May 2018).

The goal of this research is to raise awareness among European organisations regarding the new privacy regulation, and to support organisations on their journey to GDPR-compliance. If you want to know how compliant your organisation is when it comes to customer interaction, you're invited to take our online self-test.

Consent

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?

- The **United Kingdom** scores highest, **France** scores lowest.;
- **Media & Publishing** is the best scoring vertical;
- Most of the organisations fulfill some of the GDPR-requirements;
- **12.4%** is almost or fully compliant when it comes to consent.

We do see improvement in this fifth measurement. There are hardly any obversations anymore that score 'uncompliant across the board'. Overall there's a shift in the right direction.

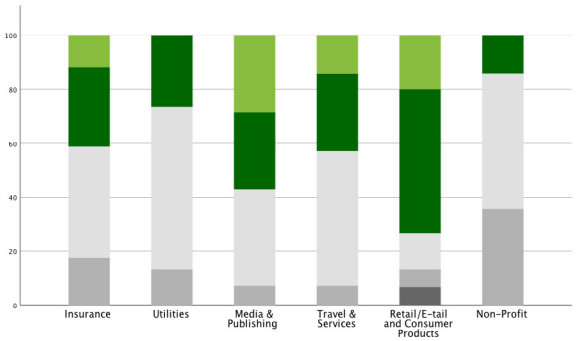
There are more observations where consent is being asked for and purpopes are given. However, the purpose of use is often not very specified, and certainly not per field. We still encounter a lot of vague descriptions, and the information is often hidden in privacy statements. We believe that is a missed opportunity. Companies now give the impression that they are more or less compliant and that they've adjusted their privacy statements, but users still are not really in control.

The United Kingdom has been scoring highest on consent since we started the survey. France is the country that has been scoring lowest since the beginning. With GDPR now being in force the French organisations in the sample only get an average score of 1.58.

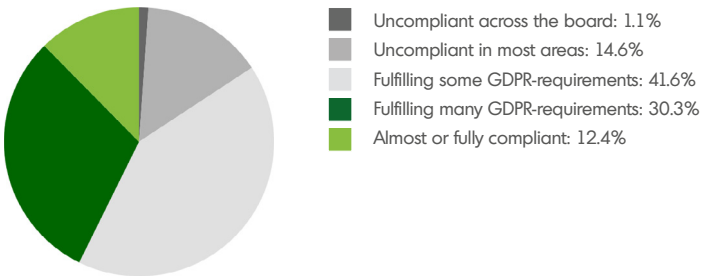
When it comes to industries, we observed some improvements in the Media & Publishing sector. With an average score of 2.79 out of 4 they are the winning vertical, followed by Retail/E-tail & Consumer Products with 2.73.

Overall, we see some misuse of the legitimate interest in relation to marketing purposes. The scope of this lawful base of processing is complicated. In some cases marketing purposes could be of legitimate interest, but we see organisations make use of this base without even asking for 'soft' opt-ins, and in vague and hidden privacy policies, to which you do not always consent during registration.

Consent score per industry (June 2018)

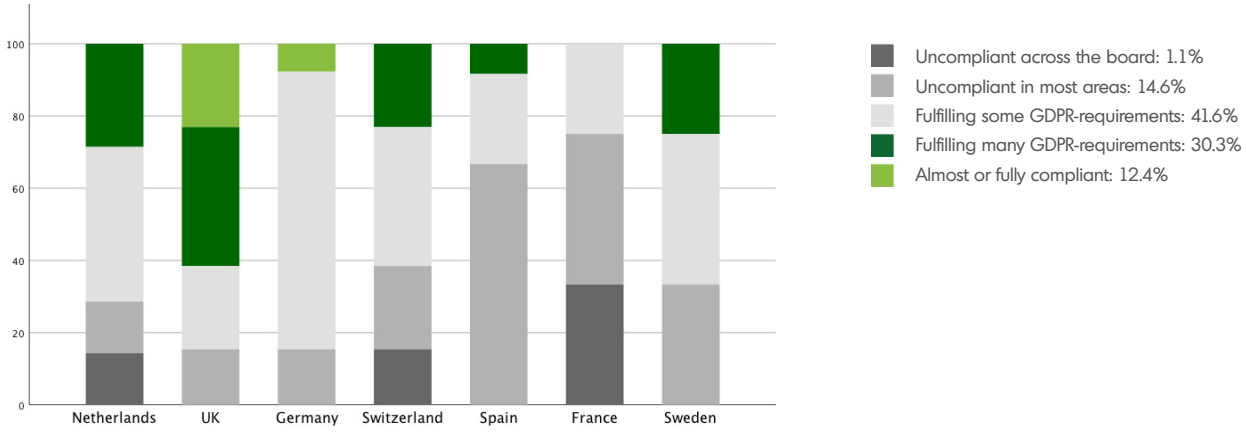


Overall score on consent (June 2018)

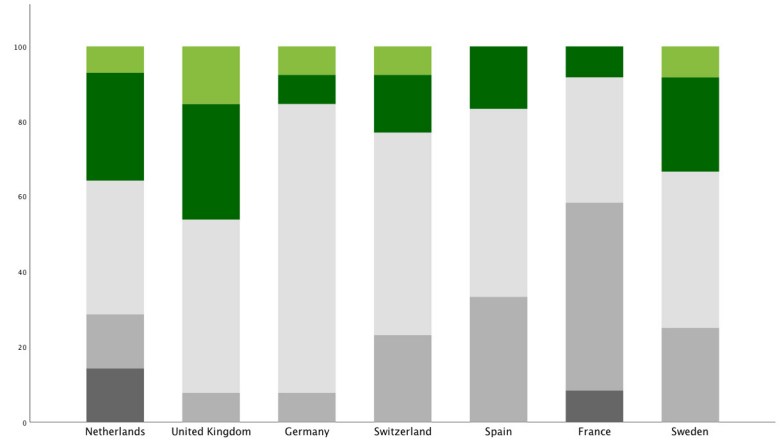


Development in consent, score per country

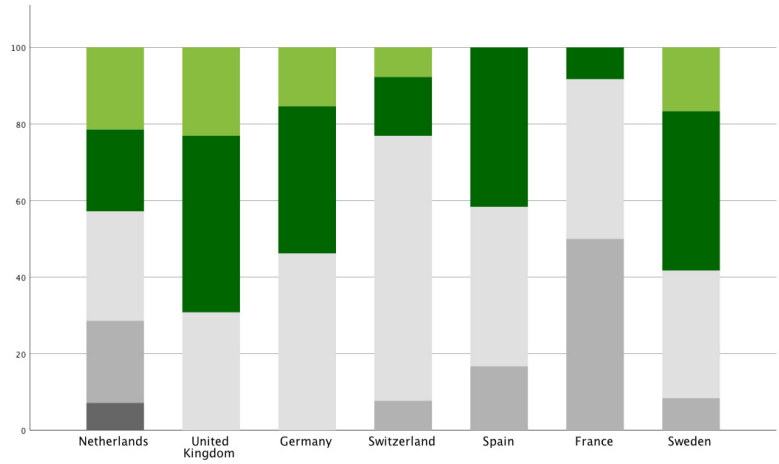
Consent score per country (November 2017)



Consent score per country (early May 2018)



Consent score per country (June 2018)



Ability to withdraw

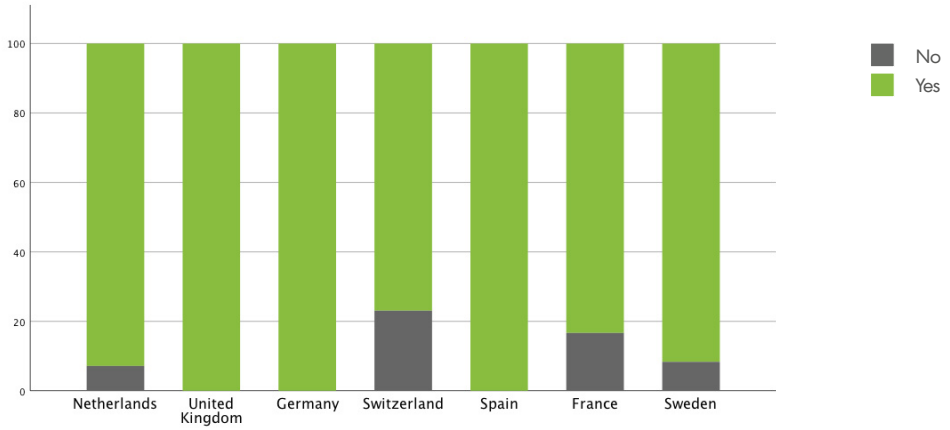
Consent must be given freely; specific, informed and unambigious. An individual must have the possibility to withdraw consent at any time, just as easy as it was given.

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

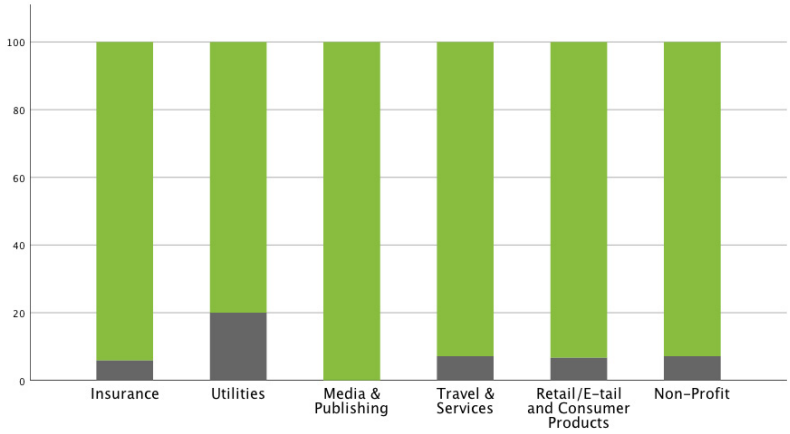
As the right to withdraw was not always present in the registration process, we also investigated the privacy statements and the procedure for revoking consent for receiving newsletters. In 7.9% of all observations the ability to withdraw was not addressed. This is a huge improvement compared to the early May measurement, where the percentage was 16.9%. In the first measurement round in November, this percentage was 34.2%. So this is really one of the variables were we observe a big improvement. The percentages align with the country graph: in 3 out of 7 countries the ability to withdraw was addressed by all the organisations in our sample.

- In **7.9%** of cases the ability to withdraw is not addressed in the registration phase nor in the privacy statement; during the previous measurement this was still **16.9%**;
- In November **34.2%** did not address the ability to withdraw.

Ability to withdraw. Score per country.



Ability to withdraw. Score per industry.



Right of access

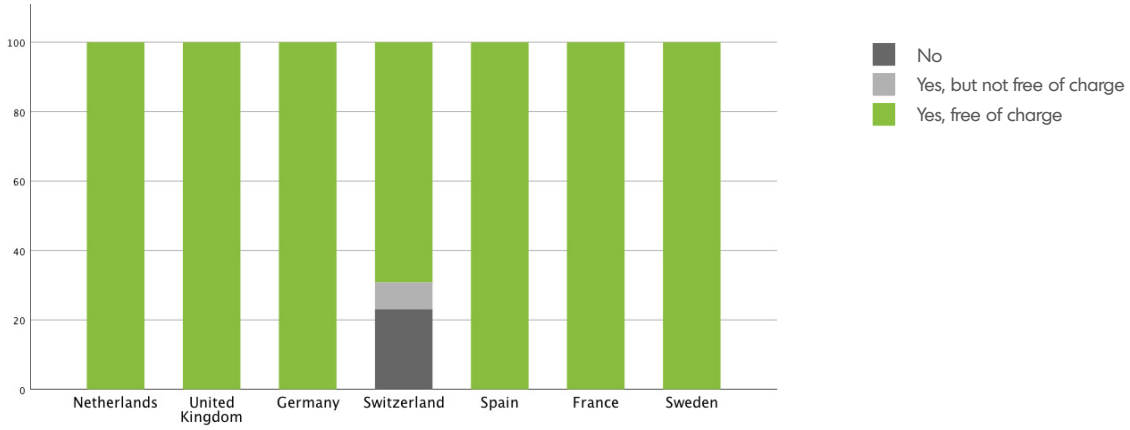
European citizens have the right to obtain information on whether or not their personal data are being processed. If that is the case, there is a right of access to that data (including amongst others the purpose of use and the envisaged period for which the personal data will be stored). Moreover, this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

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

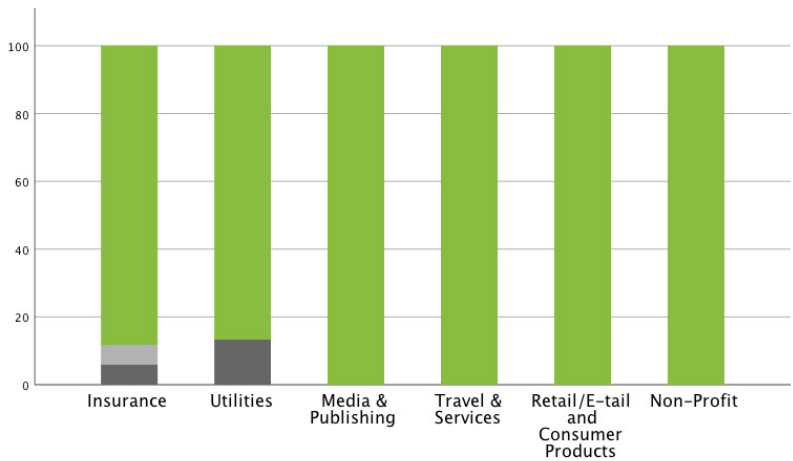
In early May we observed that 73% did provide the right of access free of charge. The other companies either did not provide the right, or provided it at an administrative fee. Especially in the UK this was custom. In the last measurement this changed. Only in Switzerland we observed organisations that do not provide access or charge a fee for providing an individual data overview. Since Switzerland is not part of the EU, they do not need to comply if they do not interact with EU citizens. However, the country did draft new privacy laws that take the GDPR into account, but these laws will be in force later this year.

- **3.4%** does not mention this right at all;
- **1.1%** provides access, but not free of charge;
- **95.5%** provides access to data.

Is the right of access mentioned? Score per country.



Is the right of access mentioned? Score per industry.



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.

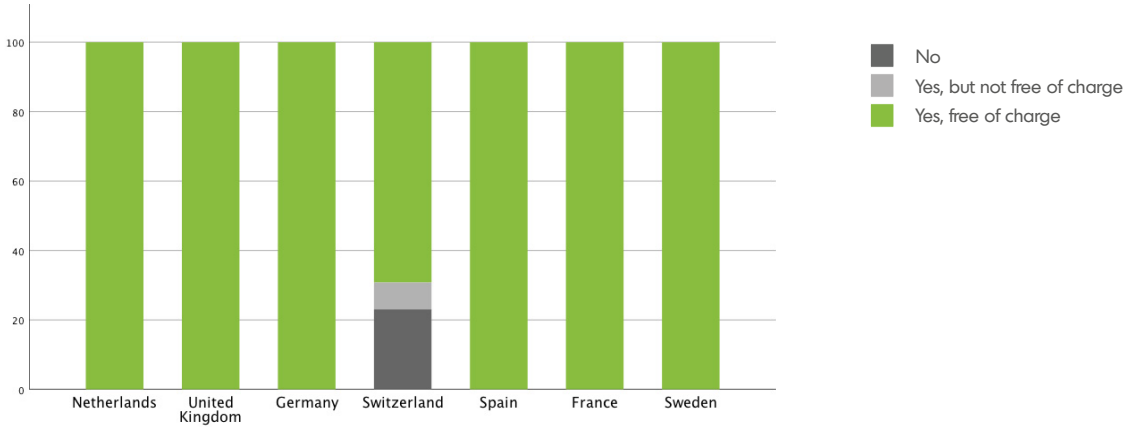
- Is the possibility for rectification mentioned anywhere?

4.5% does not mention the right of rectification at all. This is an improvement compared to the early May measurement, where the percentage was 23.6% and an even greater improvement compared to November 2017, where 31.5% did not mention this right.

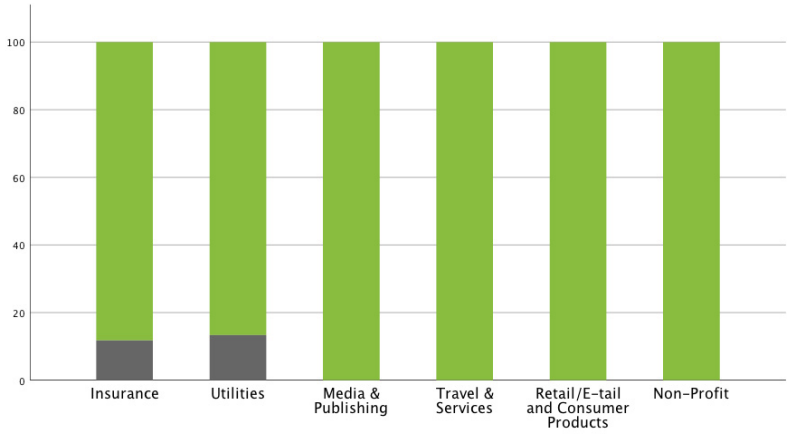
Again, only in Switzerland observations occurred where firms did not provide the right of rectification in industries 'Insurance' and 'Utilities'.

- **4.5%** does not mention the right of rectification;
- In May this percentage was still **23.6%**.

Right of rectification. Score per country.



Right of rectification. Score per industry.



Right to erasure (1/2)

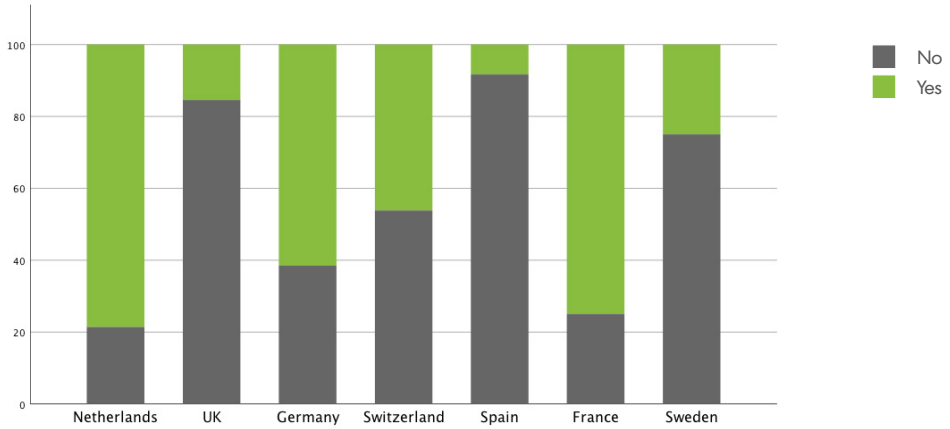
Initially known as the right to be forgotten, the right to erasure empowers consumers to demand for erasure of their personal data, unless processing is necessary for specific reasons stated in the regulation, such as compliance with law. In all other case, it must be possible for consumers to completely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

- Is the right to erasure mentioned?

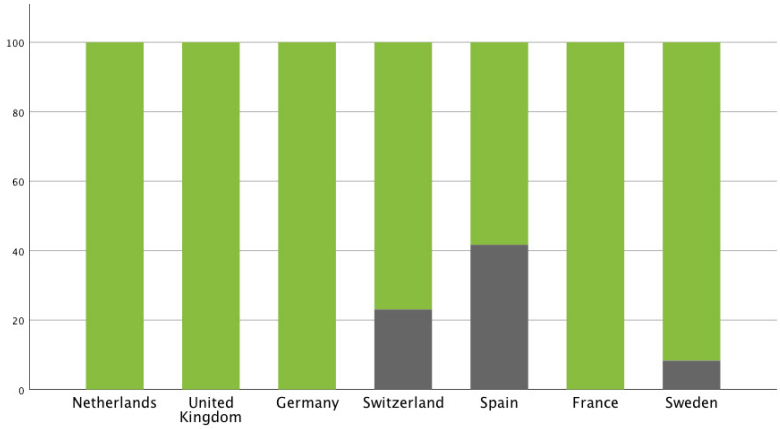
The right to erasure is one of the rights that most European countries did not yet have included in their previous legislations. In November 55.1% did not provide this right. In early May this was 50.6%, still a majority of companies. In our most recent observation we measure a very big improvement when it comes to the right to erasure. Only 10.1% does not mention this right at all. On a country score it is good to see that the Netherlands, the UK, Germany and France all have the right in place. There's still some work to do for Sweden, Spain and Switzerland.

- **10.1%** does not mention the right to erasure;
- In previous measurements this was still a majority;
- The Netherlands, the UK, Germany and France all have the right in place.

Right to erasure. Score per country (November 2017)

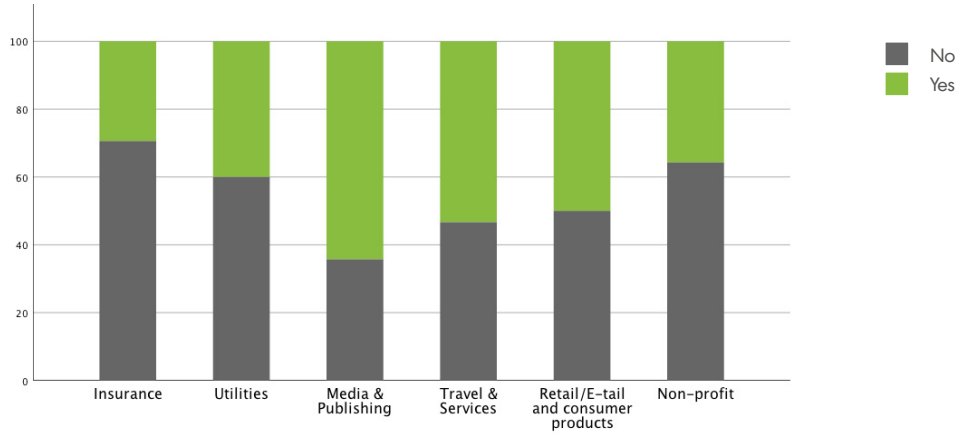


Right to erasure. Score per country (June 2018)

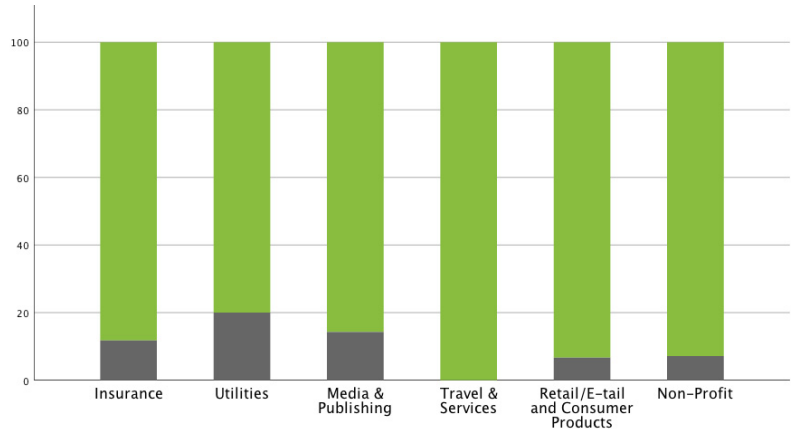


Right to erasure (2/2)

Right to erasure. Score per industry (November 2017)



Right to erasure. Score per industry (June 2018)



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.

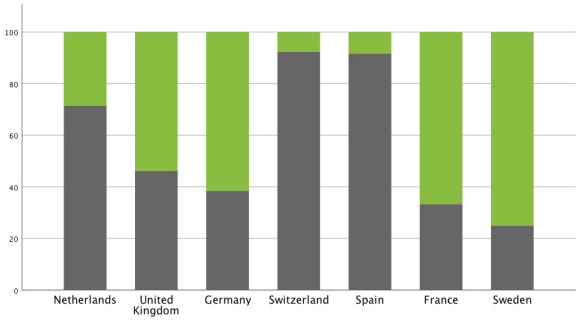
- Is the period for which consumer's data will be stored specified?

In 57.3% of all cases the firms do not specify the data retention period. Although the number did increase a lot (November 2017: 89.8%, early May: 77.5%), this is still a very high percentage. Most data controllers mention something about their retention policies, but they are not specific about the exact period that personal data is stored. Most companies use vague descriptions. This should really be a point of focus for data controllers, since the GDPR is all about transparency.

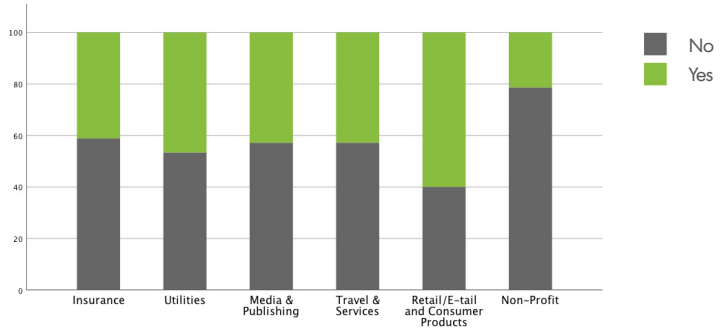
Compared to early May there have been some countries that made a lot of progress. These countries are the United Kingdom and Germany. They have gone from about 70-80% not specified to under 40% not specified. France and Sweden also made progress, they already scored best on this aspect of GDPR, but now even more firms adopt specified data retention policies.

- Only **42.7%** of all organisations specify the data retention period;
- This is already a large improvement compared to previous measurements.

Is the data retention period specified? Score per country.



Is the data retention period specified? Score per industry.



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.

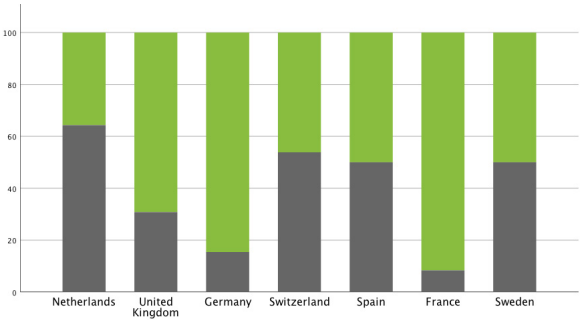
- Are there any 'pre-ticked boxes'? Can the consumer make his/her own decisions while interacting with the organisation online?

39.3% of the organisations in our sample do not act according to privacy by default. This was 46.1% in November and 42.7% in early May. The improvement is only small, which is explainable, since this is a right that most marketing departments will not be too fond off.

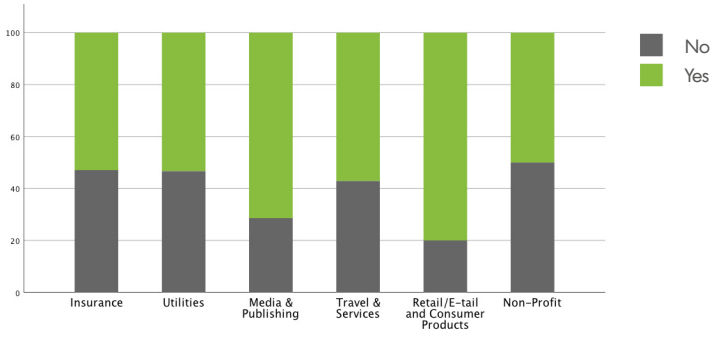
At a country level we do not see major differences compared to the early May measurement. Only the United Kingdom has taken some major steps in improving on privacy by default: from almost 60% not acting according to privacy by default to 30%. Especially in the Netherlands there were quite some observations where boxes are pre-ticked and you have to untick a box in order not to receive marketing and personal offers. This is not the way to go.

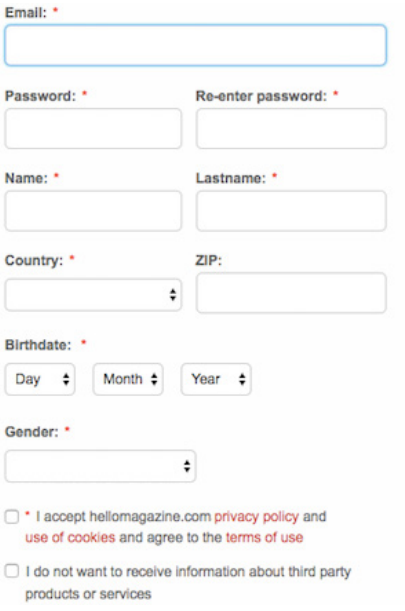
- **39.3%** does not act according to privacy by default;
- **France** scores best;
- The **United Kingdom** made the best progress;
- The **Netherlands** scores lowest.

Privacy by default. Score per country.



Privacy by default. Score per industry.





<<< 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 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 52% of firms that process sensitive data, are actually processing these data with the explicit consent of the data prospect, thus according to GDPR. This is a slight improvement compared to March, where only 46.2% was compliant when it comes to processing special categories of data. In November 2017 it was 26.9%. So, we see that some improvement has been measured, however, when it comes to sensitive data, organisations should be extra careful. Processing these special categories of data is a serious responsibility and organisations should act accordingly.

Results on a country-level

In our fifth measurement the United Kingdom scores highest on GDPR-compliance. It's the first time that they earn that title of honor. The UK was already frontrunner when it comes to consent (they scored best on consent five times in a row), but the country now also improved on other aspects. One of the elements that was remarkable in previous rounds was the right of access to personal data: in the UK it was custom to charge a fee for this overview. That has now disappeared, and under GDPR an overview of personal data is provided free of charge; a very good step!

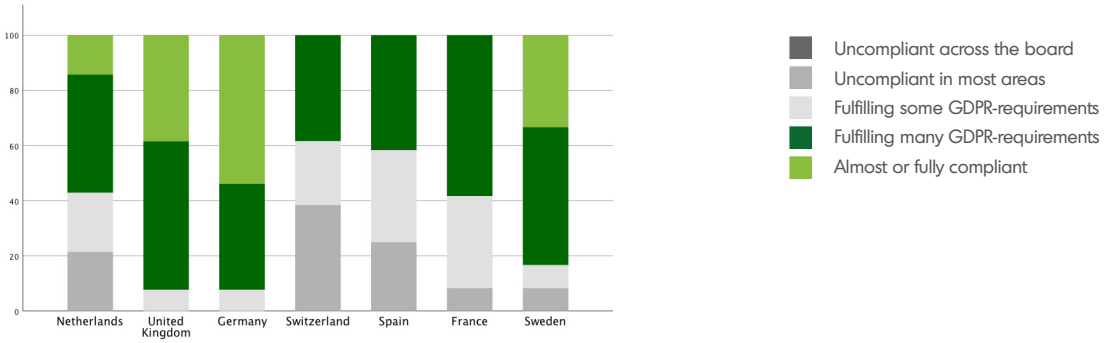
Looking at the graph per country Germany seems to score better, but the average scores in the UK are higher. Germany can still be proud with a second place. German firms are really precise in their updated GDPR-proof privacy statements. They tend to mention the GDPR article numbers they are complying to in a precise way, which shows they take their compliance seriously.

Sweden is third, and well on its way with an average score of 7.80. Joined by Germany and the UK they are still far ahead of the other countries. The Swedish organisations tend to be really transparent about how they use personal data. Their average consent score is 2.67, in combination with a very clear communication of consumers' rights.

- The **United Kingdom** scores best with an average of 8.24 out of 10;
- **Germany** & **Sweden** are second and third.

Switzerland has the lowest score, as was also the case in all previous rounds. Their average is 5.69 out of 10 compared to 4.35 in early May. They have made some progress, however, not spectacular. Although the country is not a EU member state, it did reform its own privacy laws to the same standards as GDPR. On top of that, Swiss companies operating internationally will interact with EU citizens, and therefore will need to be compliant. The current state of our Swiss sample shows that consent is rarely demanded, and privacy statements are very basic.

GDPR score specified per country



Average scores per country:

	Average GDPR-score				
Country	November 2017	January 2018	March 2018	May 2018	Post-GDPR
United Kingdom	4.96	5.26	5.41	5.40	**8.24**
Germany	5.61	5.76	5.99	6.52	**8.16**
Sweden	4.48	4.80	5.30	6.43	**7.80**
Netherlands	5.76	5.59	5.81	5.95	**6.90**
France	4.98	5.38	6.04	6.13	**6.85**
Spain	4.62	4.79	4.93	5.17	**6.29**
Switzerland	4.01	4.39	4.50	4.35	**5.69**

Results on an industry-level

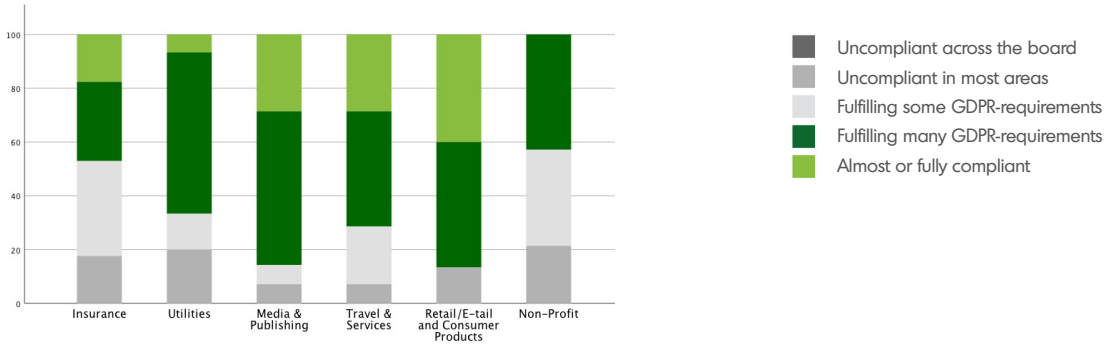
Throughout all editions of our research, Retail/E-tail & Consumer Products stood out because of the high scores they usually got. This is again the case for this measurement round, where this industry scored 8.00 out of 10. Firms in this industry usually clearly ask for consent and set out their purpose of use per feature on the website in the privacy statement. When placing an online order, it is clearly set out what data is needed under 'online orders' in the privacy statement, specified with the why and a data retention policy. They also clearly communicate the individuals' rights. This industry, that heavily depends on marketing efforts, shows that it is possible to be more or less compliant and be marketing savvy at the same time.

The Non-profit industry still has a long way to go. Although organisations in this category did improve over time, this industry was usually scoring lowest. This is mainly caused by low consent scores. The average score on consent is 1.79 out of 4.00, which is really low. Organisations also do not address the individuals' rights. Pre-ticked boxes are being used frequently, because the firms are assuming that if you donate, you want to stay updated. This makes sense but is still not according to privacy by default.

Overall, the graphs show that there is progress towards GDPR-compliance. We see more bright green at the top of the bars, which means more firms landed 'almost or fully compliant' on GDPR compliance.

- **Retail/E-tail and Consumer Products** scores best with an average of 8.00 out of 10;
- **Non-Profit** scores lowest.

GDPR score specified per industry



Average scores per industry:

	Average GDPR-score				
Industry	November 2017	January 2018	March 2018	May 2018	Post-GDPR
Retail/E-tail and Consumer Products	6.18	6.23	6.57	6.97	**8.00**
Media & Publishing	5.61	5.82	6.25	6.46	**7.74**
Travel & Services	5.49	5.55	5.81	5.94	**7.42**
Insurance	4.44	4.48	4.66	4.98	**6.86**
Utilities	4.48	4.61	4.61	5.07	**6.47**
Non-Profit	3.50	4.32	4.82	4.89	**6.36**

In conclusion; the bigger picture

This report contains the results of the fifth measurement of iWelcome's research, obtained during June 2018. The four previous measurements were taken over November 2017, January 2018, March 2018 and early May 2018.

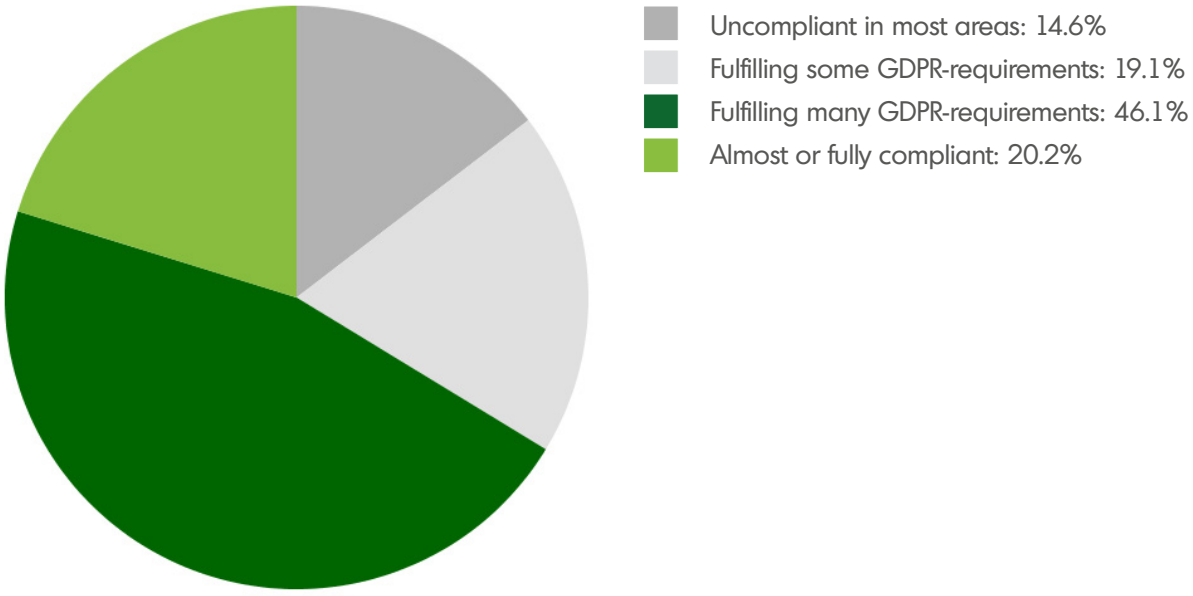
In this last measurement, the ratio has been reversed. While in early May only one third of all organisations in the sample was fulfilling many to most GDPR requirements, this is now two third. A major improvement, thanks to many renewed privacy statements and revised registration processes. From November to early May there was a slow but steady improvement of 13%, but we see now that the actual date was a real trigger to get things done.

This also means that 33.7% is still uncompliant. Some GDPR capabilities are easy to implement, and we see progress there. Most basic GDPR rights like the right of access and rectification are in place (we did not assess the ease of use for consumers, so we do not have records on that). The requirements that are more complicated and still need the most work done are consent, data retention policies, privacy by default and sensitive data.

From these results we believe there are two main conclusions to be drawn. Firstly, for a lot of companies GDPR seems to be a checklist and being compliant is just about avoiding fines. The attitude towards consumers doesn't change. GDPR feels like a burden, and not like an opportunity. Secondly, it looks like more complex issues as consent (specifically purpose of use) will need a framework of best practice before companies will invest in changing their approach. In that perspective, we are happy with initiatives as the Kantara Initiative workgroup for Consent Management Solutions, chaired by Corné van Rooij, VP Product at iWelcome.

These kinds of workgroups will hopefully set a standard that is also useful for smaller organisations. In our research, we assessed larger organisations that have resources to set up a GDPR machine, but if we would change our scope and assess smaller organisations, would the results be similar? Our general market expectation is that larger organisations will have to pave the way for the smaller ones. From that angle it is worrying that 33.7% is still uncompliant.

Overall GDPR score



What's next?

We see that large organisations have been able to implement a large part of the required changes in their customer journeys now that GDPR entered into force. Still we see that there is work to be done, especially when it comes to the more complex elements of the legislation. And GDPR often feels like a checklist, where the goal is to be compliant in order not to get fined. Whereas in our view, it is all about building trusted relationships with customers. This creates an opportunity for frontrunners to outsmart the competition by investing in empowering customers with full control over their personal data.

iWelcome's platform can support these frontrunners; it has been recognised as 'excellent' and 'innovative' for its fine grained GDPR support by analysts Gartner and KuppingerCole. If you want to know how we can help organisations to implement the key CIAM capabilities, please contact us: **sales@iwelcome.com**

"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