Central Government

Privacy Policies

How does yours measure up?

A MyLife Digital research project in association with Civica

civica digital

Transforming Services • Improving Lives

Introduction

The public places a great deal of trust in the safety and security of their personal information, especially when held by government departments and arms-length bodies (ALBs), who often collect and store citizens' personal data, including sensitive information.

The UK government has demonstrated its commitment to maintaining and improving the security surrounding personal data, most recently in December 2016 when the Department of Culture, Media and Sport published its Cyber Security Regulation and Incentives Review[1]. The review announced that the forthcoming General Data Protection Regulation (GDPR) will be a central focus on how personal information is secured.

Despite this focus, developing a consistent, government-wide approach to the protection of personal data may prove to be a challenge. In 2016, the National Audit Office reviewed the spending on ALBs by four government departments[2] – Department

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf

[2] https://www.nao.org.uk/wp-content/uploads/2016/05/Departments-oversight-of-arms-length-bodies-a-comparative-study.pdf

for Business, Innovation & Skills; Ministry of Justice; Department for Environment, Food & Rural Affairs; and Department for Culture, Media & Sport. It found that although the four departments provided £25bn of funding to 116 ALBs, there was no collective understanding of what type of oversight is appropriate and cost-effective for the different types of bodies.

This lack of a consistent approach may be cause for concern, given the public's expectation that all government departments and ALBs should not just be held to the same standards, they should be setting the benchmark in their policies and practices that all organisations should aspire to reach. Especially, in relation to how they collect, manage and secure the personal information of the citizens they serve.

Preparing for GDPR

Like every organisation, government departments and ALBs will be subject to the GDPR, which comes into force in May 2018. This regulation is a result of the desire to bring greater accountability and transparency for all organisations that collect, store and analyse personal information.

Equally, the regulation gives citizens new rights, including the 'right to be forgotten' which creates new obligations. If these regulations are not met, fines can be given up to €20million Euros.

Before the GDPR comes into play, there are practical and important steps that government departments and ALBs can take today. One of the first aspects that should be considered is a thorough review of your organisation's Privacy Policy.

Benchmark your organisation

Civica and MyLife Digital have compiled this report to help government organisations identify any gaps in their Privacy Policey, in order to prepare for the GDPR.

We've analysed the Privacy Policies of 100 government bodies and ALBs that maintain and run their own independent websites, looking at public sector organisations across education, health, care, environment, agriculture, medical, defence, finance and justice. We've researched the requirements of the GDPR and we've read the guidance from the Information Commissioner's Office (ICO) regarding their findings against organisations that have breached the current Data Protection Act 1998.

However, we are not here to give you legal advice. Every Privacy Policy should be created to explicitly state the policies of each individual body.

We have aggregated the results and presented the percentage findings based on nine different measures. Using these results could help you to:

- Make a comparison
- Find out if you are protected
- See what steps you need to take to improve your policies and processes and to increase engagement between you and your public
- Strengthen the trust they place in you.

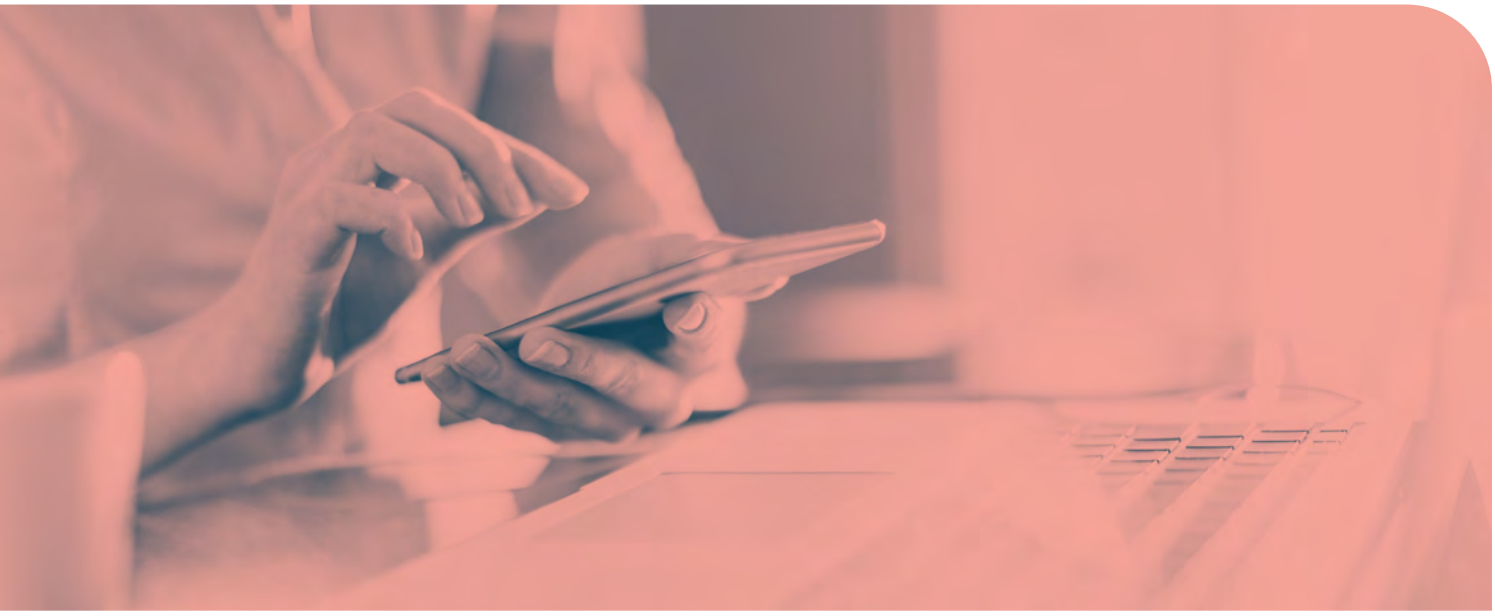
For more information about how we help central government and ALBs rethink data and improve outcomes, please contact us.

Privacy Policies and the law

A Privacy Policy sets out how an organisation collects, stores and uses personal information or data, and should be freely accessible. Any organisation undertaking these actions is required to abide by the Data Protection Act 1998 (DPA).

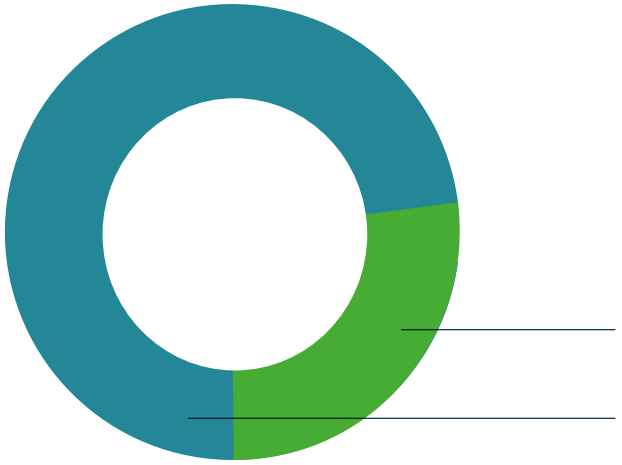
In this research, we've assessed the Privacy Policies of government departments and arms-length bodies who maintain their own website against the following nine measures:

1. Do you have a Privacy Policy?
2. Is your Privacy Policy easy for the public to find?
3. Does your Privacy Policy mention the collection of personal data?
4. Does your Privacy Policy mention profiling?
5. Does your Privacy Policy reference sharing of data?
6. Does your Privacy Policy include how data will be used?
7. Does your Privacy Policy mention how you collect data?
8. Does your organisation give details of how long data is kept on record?
9. Do you include a Data Controller or Processor contact?



The results

1. Do you have a Privacy Policy?



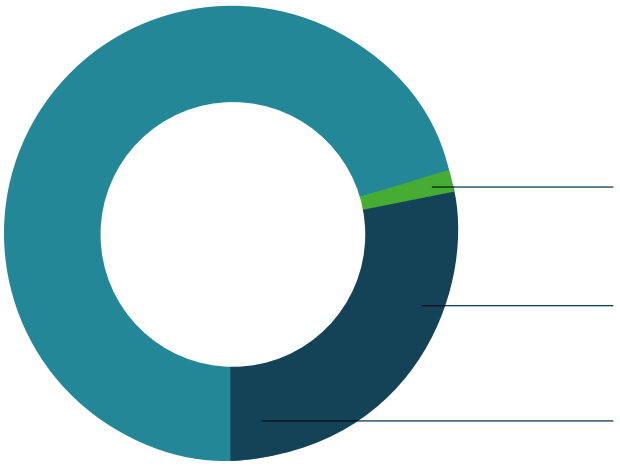
All organisations should have a data protection and information security policy that details their own processes and procedures about what information they collect, how they protect, manage and secure all personal information.

Our research discovered that, very surprisingly, less than three quarters of the organisations we looked at published a Privacy Policy on their website. This is the lowest figure from all research conducted, including local authorities, housing associations and charities.

28% No

72% Yes

2. Is your Privacy Policy easy for the public to find?



Privacy Policies should be readily accessible online for the public. The Data Protection Regulation stipulates that if you're only collecting data for specified purposes, you need to notify users through your Privacy Policy and that "they can access your Privacy Policy easily".

Our team of researchers went in search of Privacy Policies and found they had to work to find a third of them. Only 68% of organisations made it easy for the public to find their policy. This is the lowest figure of all the sectors that were researched.

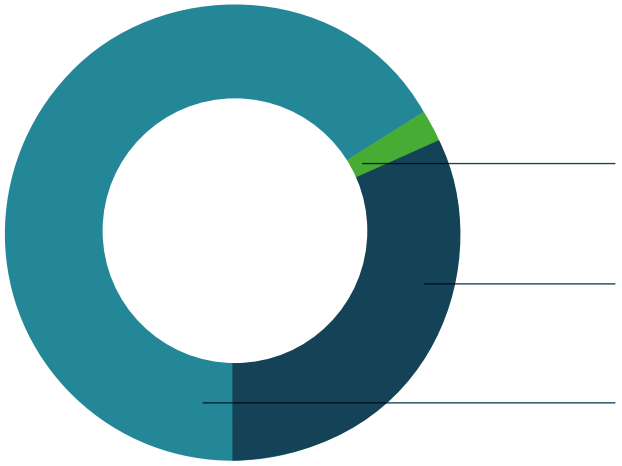
3% Not at all easy

29% Quite easy

68% Very easy

3. Does your Privacy Policy mention the collection of personal data?

The collection of personal data is one aspect the ICO particularly scrutinises. Of those government bodies and ALBs that have Privacy Policies, over one third do not reference that they collect personal information, leaving these organisations once again trailing behind other sectors.



4% Vaguely mentioned

34% Not mentioned

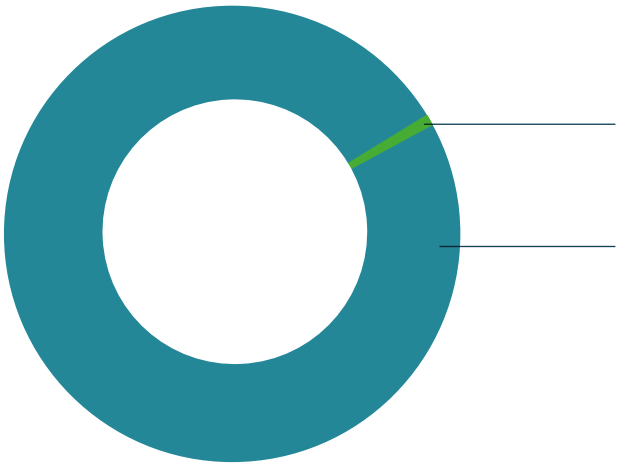
62% Clearly stated

4. Does your Privacy Policy mention profiling?

The use of profiling is one area of data analysis that can be misconstrued. Profiling should be about effective communication with the public by presenting them with the right message, at the right time.

The ICO expresses that you need to be transparent about the personal information you collect. Especially if you use it for insight by adding to it with other consented publicly available information.

98% of government departments and ALBs do not include any mention of profiling in their Privacy Policy. Both existing and forthcoming regulations are forcing organisations to be transparent about the personal information they collect.



2% Clearly stated

98% Not mentioned

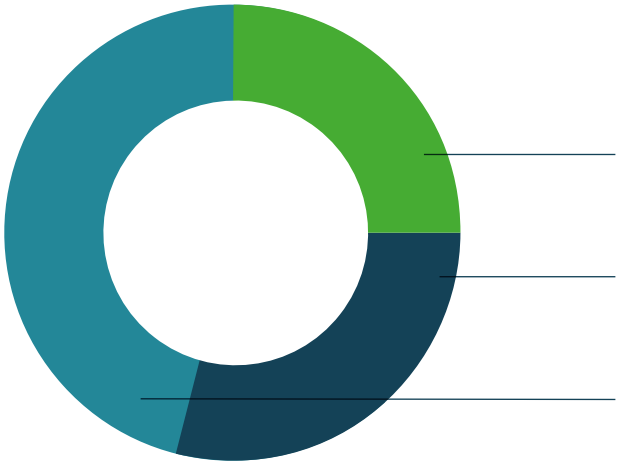
5. Does your Privacy Policy reference sharing of data?

Policies and processes regarding the sharing of data between organisations is an important element of a Privacy Policy. In the Information Commissioner's Office 'Data sharing code of practice'[3], they are clear:

"Most public sector organisations, other than government departments headed by a Minister of the Crown (which have common law powers to share information), derive their powers entirely from statute – either from the Act of Parliament which set them up or from other legislation regulating their activities."

Yet the NAO research highlighted discrepancies in the oversight by government departments of the ALBs they fund, which raises questions about the consistency of their data sharing policies.

In our research we found that only 30% of organisations clearly referenced the sharing of data.



25% Vaguely mentioned

30% Clearly stated

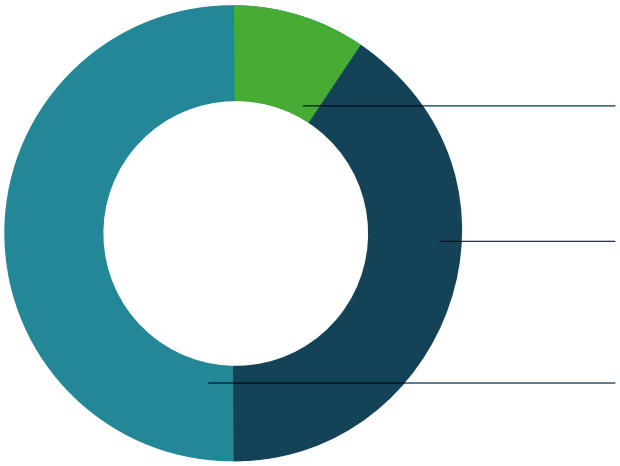
45% Not mentioned

[3] https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

6. Does your Privacy Policy include how data will be used?

As the government and ALBs prepare for the GDPR next year, we thought it would be useful to look at what practices and policies need to be in place for the 25th May 2018. One of the fundamental principles of the GDPR is including how data will be used. This overlaps with current legislation and the ICO rulings.

This is more than preferences for communication use – it covers the use of personal data, anonymised or identified, in research, for insight and for service provision.



13% Vaguely mentioned

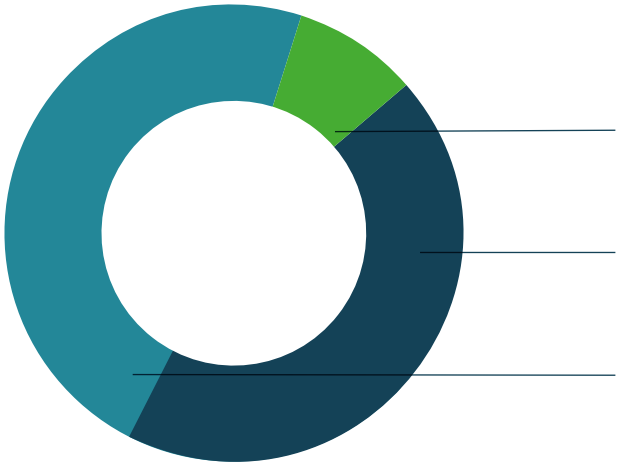
38% Not mentioned

49% Clearly stated

7. Does your Privacy Policy mention how you collect data?

In the past, how data was collected was relatively straightforward. However, as the number of channels of communication continue to gather momentum, so has our potential to gather data from multiple sources.

While this is useful for organisational efficiency, it is an area that raises the most concern with the public. Transparency about how data is collected is essential.



11% Vaguely mentioned

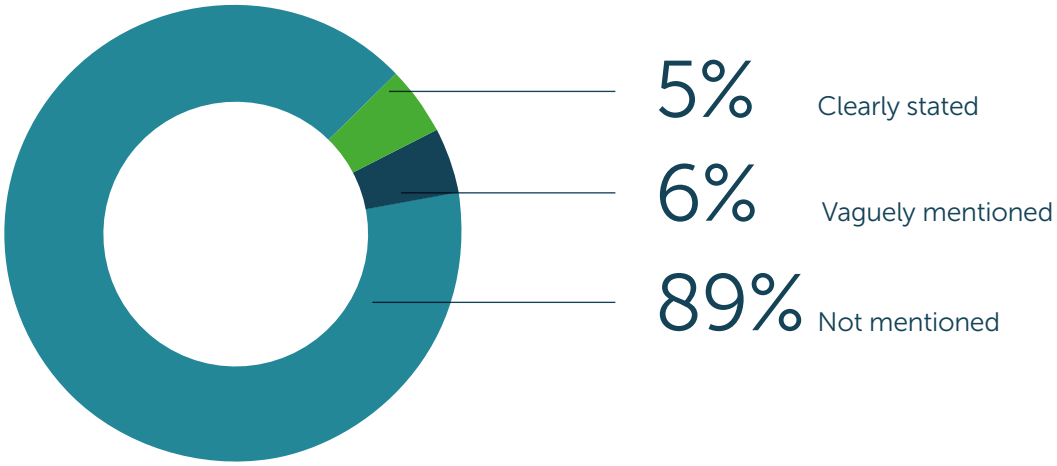
43% Not mentioned

46% Clearly stated

8. Does your organisation give details of how long data is kept on record?

The current regulation and guidance from the ICO says data should be retained for "no longer than is necessary for the purpose you obtained it for". Research from Data IQ[4] in 2016 showed that 21% of consumers believe that consent is only valid for 6 months.

While this enables data to be disposed of, it does present a challenge for all organisations, including Government bodies and ALBs. They need a system that allows for the stamping of when consent for data was obtained, and therefore allows the safe and secure disposal of data. This element is key for the new GDPR. It is essential that organisations consider how long they retain this data and can verify this period has been considered and documented.



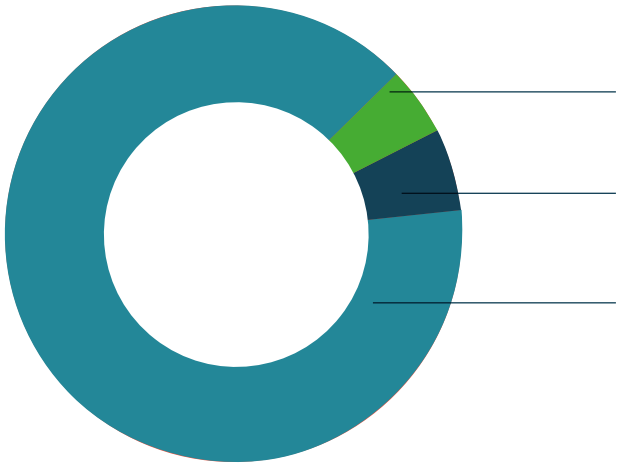
[4] https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

9. Do you include a Data Controller or Processor contact?

This is one of the most significant changes of the new regulation. Under the GDPR, government departments and ALBs must have one.

In our research, 86% of organisations did not include a named data controller or processor.

By naming a controller or processer, government departments and ALBs need to be aware that sanctions can be brought against the controller and the processer of data, as well as the organisation itself.



5% Vaguely mentioned

9% Clearly mentioned

86% No contact given

Privacy and trust

We hope that our research will help you to identify the gaps, if you have them, in your own policies and procedures. It sets out the requirements as they currently stand and what government bodies and ALBs need to do in preparation for the GDPR.

In May 2018, all organisations will need to show:

- What data has been collected?
- Why is the data being collected and its purpose?
- Who is using the data?
- When was the permission granted or changed (date)?
- Where was the permission granted (source)?

These measures focus on compliance, as there is a considerable risk to government bodies and ALBs if they get it wrong. While compliance is important it should only be the baseline, not the aspiration.

Complying with GDPR is inevitably going to involve increased work, time and cost in implementing strategies and processes to comply. Yet, if done in the right way, the opportunity it creates to build or strengthen trust could well outweigh these issues.

Trust can mean many things, from transparency of how much a CEO is being paid, the security of personal information, how services are being tendered, to how government bodies and ALBs share data.

Now is the time not just to protect your organisation, but to go a step further; to build and deepen the trust your public have.

Improving your consent capturing procedures and updating your policies will provide you with an excellent opportunity: an opportunity to seek the public's permission; an opportunity to engage at a deeper level; an opportunity to create a value exchange where both the public and your organisation benefits; an opportunity to demonstrate the positive impact that you're making to the country and the people.

Research partners

Civica Digital

Civica Digital (www.civica.com/digital) provides organisations which deliver essential services with complete digital solutions, from strategy consulting and solution design to software development and ongoing managed services. With in-depth business and technology know-how founded on creating secure business-critical systems, our user-centred approach starts with customer needs, putting insights, data and strategic thinking in the driving seat.

Supporting 500 customers across government, public safety, health care, travel & transport, financial services and other regulated markets, we are the trusted partner to deliver design-driven digital transformation.

Our team of experienced business analysts, consultants and digital specialists can help you fully understand the impact of the incoming GDPR on your organisation. We'll help you identify gaps and risks and formulate a roadmap for compliance, that will not just remove the uncertainty around GDPR, but enable you to deliver better outcomes and build trust with your customers.

Civica Digital is part of the Civica Group, a market leading specialist in business-critical software, technology and outsourcing services that help teams and organisations around the world to transform the way they work.

MyLife Digital

MyLife Digital's (www.mylifedigital.co.uk) mission is to empower organisations & individuals to realise the meaning, value & power of their data. The propositions enable organisations to rethink their consumers' personal data to deliver change.

With existing analytics practices in Charity and Elite Sport, and now plans to move into Healthcare, Defence & Local Government, MyLife Digital has built a digital application platform to deliver innovative cloud-based services to these sectors.

The Consentric® platform connects organisations to individuals to generate informed insight from informed consent. The services both help organisations comply with data protection obligations and build deeper, more trusted relationships with their consumers, employees or citizens.

Further information

Richard Page
Sales Director
Civica Digital
07973 886 641
digital@civica.co.uk
www.civica.com/digital

James Bagan
Sales Director
MyLife Digital
01225 636 280
jbagan@mylifedigital.co.uk
www.mylifedigital.co.uk