PUBLIC UNDERSTANDING OF GDPR

How companies, regulators, and civil society can support data protection rights

Ed Johnson-Williams
Open Rights Group

January 2019

About
Open Rights Group

As society goes digital we wish to preserve its openness. We want a society built on laws, free from disproportionate, unaccountable surveillance and censorship. We want a society in which information flows more freely. We want a state that is transparent and accountable, where the public's rights are acknowledged and upheld.

We want a world where we each control the data our digital lives create, deciding who can use it and how. We want the public to fully understand their digital rights, and be equipped to be creative and free individuals. We stand for fit-for-purpose digital copyright regimes that promote free expression and diverse participation in culture.

We campaign, lobby, talk to the media, go to court — whatever it takes to build and support a movement for freedom in the digital age. We believe in coalition, and work with partners across the political spectrum.

We uphold human rights like free expression and privacy. We condemn and work against repressive laws or systems that deny people these rights. We scrutinise and critique the policies and actions of governments, companies, and other groups as they relate to the Internet. We warn the public when policies — even well-intentioned ones — stand to undermine the freedom to use the Internet to make a better society.

openrightsgroup.org

Written by Ed Johnson-Williams
Policy and Research Officer
Open Rights Group

Set in Lato, available under a SIL Open Font License v1.10
www.fontsquirrel.com/fonts/lato

Open Rights is a non-profit company limited by Guarantee,
registered in England and Wales no. 05581537

Open Rights Group, Unit 7, Tileyard Acorn Studios, 103-105,
Blundell Street, London, N7 9BN

Registered Office: 12 Duke’s Road, London WC1H 9AD

Introduction

Debate and guidance about data protection and the General Data Protection Regulation (GDPR) has focussed on helping businesses achieve compliance. This is clearly valuable. The strengthened rights that individuals enjoy under GDPR have, however, received less attention.

Important questions are left to be explored relating to the public understanding of data protection. How aware is the public about data protection and what their rights are? If they are aware of their rights, how well do they understand what those rights entail? Where do these rights fit within people's everyday lives?

Open Rights Group has carried out research over the last year to investigate these questions. We have also created a website with Projects By IF called *Data Rights Finder*.[1] On *Data Rights Finder*, we present analyses of organisations' privacy policies to make it clearer how they use data and make it easier for people to make requests to organisations using their data protection rights. As a starting point, we focussed on providing information about the main banks, insurance providers, comparison websites, and financial services organisations.

This report explores the findings from our research and our experiences of creating *Data Rights Finder*. We first discuss interviews that we carried out with members of the public to build a better understanding of how aware people are about data protection and their rights. We then use our research findings and our experience of creating *Data Rights Finder* to make recommendations to regulators and civil society organisations about how to communicate well about data protection, rights, and GDPR. Finally, we look at how organisations who use data can support the data protection rights of their users, members, customers, supporters, subscribers and so on.

[1] Data Rights Finder – https://www.datarightsfinder.org

RESEARCH METHODS

Over the course of this project, we have carried out three rounds of qualitative, interview-based research. To our knowledge, we avoided speaking to people who are data protection experts, digital rights activists, or Open Rights Group members. Desk-based research and our experiences of creating a website that includes our analysis of privacy policies also inform the findings of this report.

The first round of interview research started in June 2018. To help us understand how people think about data protection and how data about them is used, we interviewed eight people. We spoke to three women and five men with a range of ages and careers. We screened our interviewees to ensure we did not talk to data protection experts. The interviews were carried out over the phone and lasted between 20 and 30 minutes each. We used a semi-structured approach to the interviews which means that we covered the same topics in each interview, but we varied the order and phrasing of the questions. This helped us to keep a natural conversation and elicit useful insights about what our interviewees thought about data protection.

We carried out usability testing of the website *Data Rights Finder* in September 2018. *Data Rights Finder* is a website that provides information about how companies use data and helps people contact companies to use their data protection rights. The website is discussed in more detail later in the report. In this research, we wanted to find out how people used the website by observing them while they carried out tasks on the site. We wanted to find the most important things to improve on the website and test assumptions we had about the reasons people would use the site. We carried out six usability tests – three of those were in-person and three were remote over video-conferencing. We spoke to a chef, a retail worker, a housewife, two academics, and a vicar. They lived in three different places in the UK. Four of them were in their 30s, one was in their 50s and one was in their 60s. This is a useful methodology for quickly discovering the easiest-to-find usability issues with a website.

In December 2018, we carried out user research to improve our understanding of people's experiences of the insurance sector and to test assumptions we had about a potential website. We wanted to find out how people thought about the way insurance companies decide whether to offer coverage or not. We also wanted to see how people feel when automated decisions are made that affect their lives. We carried out four semi-structured interviews that lasted around 25 minutes each. Three of the interviews were carried out over the phone and one was in-person. The people we spoke to were in various careers including academia and publishing. Three people we spoke to were in their 30s and one was in their 60s.

Clearly, further research would be needed to draw fully generalised conclusions about these issues. Due to restrictions of time and resources, we have interviewed a small number of people in this project. The people we spoke to cannot be said to be a representative sample of the British public. We favoured quickly capturing small amounts of relatively rich data through interviews which gave us deeper insights into how people thought about these issues. We decided against quantitative alternatives such as a survey which would have presented challenges in acquiring a deeper understanding of the views of the people involved in our research. The research was carried out within a six month period with three rounds each lasting four to ten days. As a result, this is not longitudinal research; we captured a snapshot of viewpoints. We encourage other researchers to explore the issues we discuss here at a greater scale and over a longer period. There is a basis for future work within this research.

SECTION 1

How people understand data protection and their rights

KEY POINTS

Open Rights Group research indicates that:

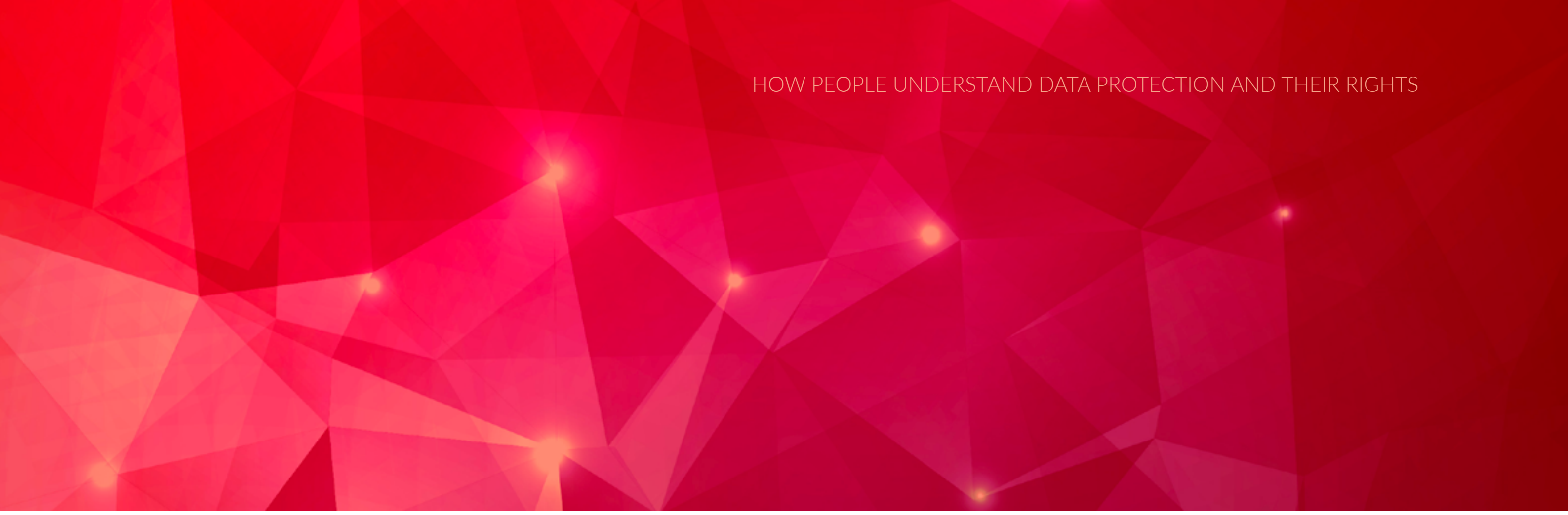
1. **The British public's awareness of their data protection rights is low.** When people become aware of the data protection rights they have, they are surprised that they have those rights. This means that people are unaware of their options when they want to resolve an issue relating to data about them.
2. **Awareness of consent as a basis for collecting and processing user data is relatively high.** The other bases for processing data are not well-known. Although awareness of consent is high, understanding of what it means is low. People are unlikely to understand when consent is or is not required to collect or use data about them. This leaves people more vulnerable to user interface designs that nudge them towards choices that are more privacy-intrusive.
3. **People do not think about their lives in terms of the rights they have.** They experience contexts and situations in their lives where they want to do something, solve a problem, improve something in their life, stop something happening to them, and so on. The rights people have will sometimes be useful or vital in those situations. This suggests that communicating to people about rights without examples of the context in which they could be applicable is unlikely to be useful to most people.

AWARENESS OF DATA PROTECTION RIGHTS IS LOW

The General Data Protection Regulation (GDPR) and the UK's Data Protection Act 2018 provide people with data protection rights. These are not all new rights. Some of them have existed since the 1995 Data Protection Directive, enacted in the UK as the Data Protection Act 1998. There are caveats to all of the rights, but in summary,[2] they are:

1. **The right to be informed** about the collection and use of your personal data. This includes the purposes for processing the data, how long it will be retained for, and who it will be shared with.
2. **The right of access** to a copy of personal data held about you
3. **The right to rectify** inaccurate or incomplete personal data
4. **The right to erasure** of personal data
5. **The right to restrict processing** of your personal data, which limits how an organisation can use your data
6. **The right to data portability** which entails allowing people to request a re-usable copy of their personal data which they can transfer to another service
7. **The right to object** to the processing of your personal data

[2] These rights are described in greater detail on the Information Commissioner's Office website: https://ico.org.uk/your-data-matters



8. **Rights in relation to automated decision-making and profiling** including a) the right not to be subject to a solely automated decision that has a significant impact on you, b) the right to specific information about automated decision-making and profiling, and c) the right to challenge and request a review or explanation of automated decisions

As part of a previous report,[3] Open Rights Group conducted research interviews with eight people in the UK to help us get some insight into whether they were aware of or understood these data protection rights. One of our findings was that awareness of these rights among the people we spoke to was very low. Generally speaking, people did not know that they had legal rights, for example, to get a copy of their data or to have data about them erased. The people we spoke to indicated they would contact an organisation if they thought that organisation had made a mistake relating to their data or if they wanted to complain. They were not necessarily aware of what their rights would be when they complained, however. This could leave them at a disadvantage to the organisation in a complaints procedure as the organisation would be more likely to have greater awareness of data protection law and the individual would be unlikely to be aware of what their legal rights afford them.

Open Rights Group has also carried out other research suggesting that awareness of data protection rights is low. We worked with Projects by IF to release a website called *Data Rights Finder*[4] in June 2018. *Data Rights Finder* helps people understand how companies use personal data and to make requests using their data protection rights. Our starting focus has been on the main banks, insurance providers, comparison websites, and financial services organisations.

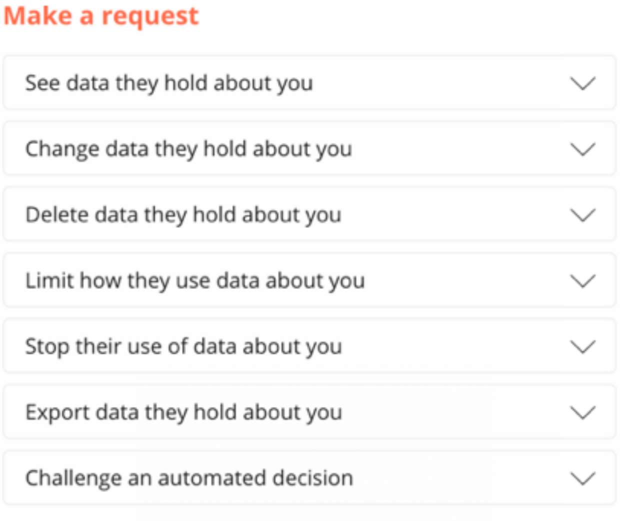
Many organisations are not making it easy enough for people to understand how their data is being used. To help address this problem, we analysed the 'privacy policies' of around 40 companies to pull out the details we thought would be important to somebody trying to understand how a company was using data. We also put together the best contact details we could find for each organisation and provided a message template to help people use each of their data protection rights when they contact an organisation.

Open Rights Group carried out usability research to see how people used *Data Rights Finder*. We showed the website to six people with varied career backgrounds, genders and ages, asked them for their impressions on the homepage and the site in general, and asked them to perform some tasks with the site like 'Find out which organisations your bank shares data with' and 'Ask Paypal for a copy of the data they hold about you'.

[3] Open Rights Group, *Debates, awareness, and projects about GDPR and data protection*. – https://www.openrightsgroup.org/about/reports/debates-awareness-and-projects-about-gdpr-and-data-protection

[4] Data Rights Finder – https://www.datarightsfinder.org

All of the people we observed using *Data Rights Finder* arrived at the section displayed in the image below. The site helps you contact an organisation. Organisations, especially larger ones, often have different contact methods for each data protection right: *subjectaccess@organisationname.co.uk* versus *erasure@organisationname.co.uk*.

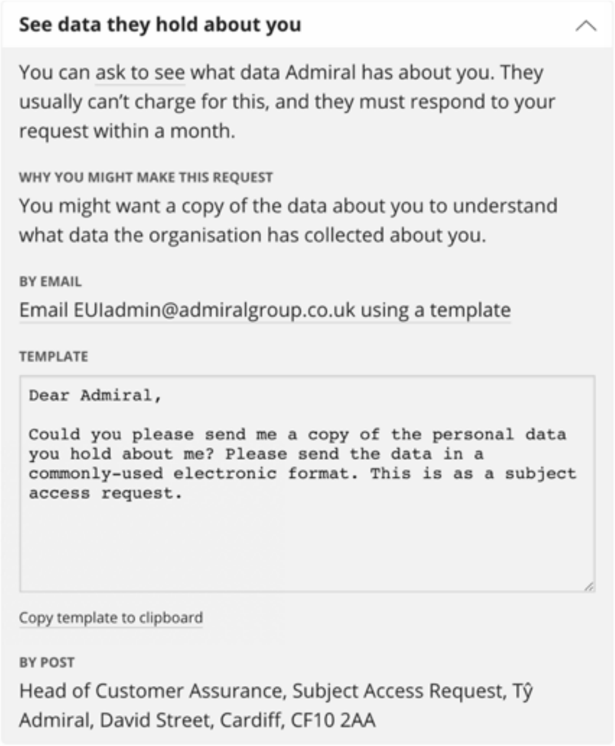


Make a request

- See data they hold about you
- Change data they hold about you
- Delete data they hold about you
- Limit how they use data about you
- Stop their use of data about you
- Export data they hold about you
- Challenge an automated decision

A screenshot from datarightsfinder.org showing the data protection rights a user could use when contacting an organisation – Ed Johnson-Williams

When a user clicks on one of the dropdown sections, it reveals a brief description of the legal right (including a link to a fuller explanation of the right), an example of why you might want to use the right, and the best contact methods we could find for the organisation. All but one of the people who took part in the usability testing clicked on at least one of these dropdown sections.



See data they hold about you

You can ask to see what data Admiral has about you. They usually can't charge for this, and they must respond to your request within a month.

WHY YOU MIGHT MAKE THIS REQUEST

You might want a copy of the data about you to understand what data the organisation has collected about you.

BY EMAIL

Email EUIadmin@admiralgroup.co.uk using a template

TEMPLATE

```
Dear Admiral,

Could you please send me a copy of the personal data
you hold about me? Please send the data in a
commonly-used electronic format. This is as a subject
access request.
```

Copy template to clipboard

BY POST

Head of Customer Assurance, Subject Access Request, Tŷ Admiral, David Street, Cardiff, CF10 2AA

A screenshot from datarightsfinder.org showing an example of how a user could contact an organisation through the site – Ed Johnson-Williams

The usability testing helped us to understand how easy the site was to use. For the purposes of this report, the most important finding was that people were surprised that they had these kinds of rights over data. After seeing these options, one person said, "Many of these are things I wouldn't have realised I could do." Sometimes they knew they could do these things, but not that it was a legal right. This revealed a lack of general awareness of the rights contained within GDPR.

HIGH AWARENESS BUT LOW UNDERSTANDING OF CONSENT IN GDPR

After several rounds of research, Open Rights Group is yet to talk to a member of the public who is clear on what their data protection rights are under GDPR. However, most people we spoke to had heard of GDPR. This had, in nearly every case, been through emails sent by organisations to refresh consent to remain on a mailing list or to announce updated privacy policies in the lead-up to GDPR coming into force in May 2018. Because of this, nearly all of the people we have spoken to have only really thought about GDPR as a law that requires consent to process data. This is not accurate, but it is likely that this is common. Further research would be required to confirm this. We first wrote about this in an earlier research report *Debates, awareness, and projects about GDPR and data protection*.[5]

In general, the people we spoke to believed that organisations should get explicit and informed consent to collect and process data. Below is a good example indicating the sentiment we heard:

> *"Well I just think it's explicit agreement to say from our side [companies'] 'This is what we're going to do XY and Z with your data.' and from your side [individuals'] 'Are you happy with this? If yes, great. If no, then we won't do XY and Z with your data.' And I think something as explicit as that would have been a good idea."*

We found very low awareness of the other legal bases for processing data under GDPR such as *performance of a contract* or *legitimate interest*. This is understandable, as when an individual's data is processed under those legal bases, they are unlikely to have been actively engaged in that processing. This has led to some of the people we spoke to believing that consent should be sought for every type of data processing. This included, for example, employers keeping records about employees. This should not require consent. We also saw some confusion around whether clicking a checkbox to confirm that you have read a privacy policy means that you have given consent to the processing detailed within that policy.

Other research by the Norwegian Consumer Council[6] has shown how Facebook and Google used manipulative user interface design and language to nudge users towards privacy-intrusive options in the lead up to GDPR coming into force. The research questioned whether "consent given under these circumstances can be said to be explicit,

[5] Open Rights Group, *Debates, awareness, and projects about GDPR and data protection*. – https://www.openrightsgroup.org/about/reports/debates-awareness-and-projects-about-gdpr-and-data-protection

[6] Norwegian Consumer Council, *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

informed and freely given."[7] There is the issue about whether giving up access to your email account or main social media presence if you refuse to consent to your data being processed is fair. Putting that aside for the moment, the Norwegian Consumer Council findings are not surprising given the low levels of public awareness of data protection law and the rights individuals have. It seems likely that at least part of Facebook and Google's success in retaining high consent rates[8] in the era of GDPR relied on low levels of awareness about what the conditions for consent are within GDPR. Those conditions for consent under GDPR are that an individual makes "a clear affirmative act establishing a freely given, specific, informed and unambiguous indication" that they agree to an organisation processing personal data relating to them.[9]

Returning to our research, some of the people we spoke to made fascinating links between asking for consent and, variously, *political correctness*, *politeness*, and *transparency*. The linking of these values with consent as a data protection concept suggested that people saw a kind of morality in how organisations went about handling their data. To summarise, we understood people as saying that 'good' organisations were honest, respectful, and open about how and why they used data. 'Bad' organisations were manipulative, secretive, and did not treat people whose data they handled with dignity. We did not find any solid evidence that people do not care about privacy or control of personal data.

These findings are from interviews and analysis carried out by an employee of Open Rights Group with a small group of participants. There would be great benefit in pursuing this avenue of research on a greater scale with independent analysis.

DATA PROTECTION RIGHTS AND EVERYDAY LIFE

Through our conversations with people in research interviews and in usability testing sessions of the *Data Rights Finder* website, it became clear that people do not go about their everyday lives thinking about daily events as having relevance to data protection. People are not routinely mapping their data protection rights on to the contexts and situations they experience.

The major exception to that was with the way people talked about the *Cambridge Analytica* story. We did not bring up *Cambridge Analytica* in our questions or framing of the conversations. Despite this, many people we spoke to talked about *Cambridge Analytica* in passing and some of them some delved into what they thought the effects of it have been. People understood *Cambridge Analytica* as being a company that carried out society-wide manipulation of individuals that relied on misuse of data about them. The people who spoke in greater detail about *Cambridge Analytica* saw it as a story about power imbalances and secretive or unseen manipulation of the public. As an example, one person said,

> *"People don't like being confronted with the idea that maybe their actions weren't entirely what they would have been. They don't like knowing they've been manipulated."*

[7] Ibid, pg 4

[8] WhoTracks.me, *GDPR - What happened?* – https://whotracks.me/blog/gdpr-what-happened.html#third-party-services-the-winner-takes-it-all

[9] Recital 32 of GDPR says, "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement."

Besides the *Cambridge Analytica* story – which was a society-wide issue rather than something specific to only them personally – the people we spoke to did not, in general, think about data protection issues as part of their everyday lives. A good example of this was someone we spoke to as part of the usability research of *Data Rights Finder*. When asked whether they would ever read a 'privacy policy' in their day-to-day life, they answered,

> *"Probably not... Unless I had an issue, I probably wouldn't go looking for it."*

If they did not have a specific issue with an organisation, they would not read a 'privacy policy'. This is not the same as saying they did not care about how their data was used. Instead, they just did not have the time and energy to read a long, complex legal document for every organisation that presents them with a 'privacy policy'.

We learned a number of things from the usability testing. One, as discussed earlier in this section, was that awareness of data protection rights is low. Another was that when people had a problem with a bank, insurance company, or financial institution relating to data about them, they would be likely to contact that company to resolve the issue. They would not necessarily realise, however, that a) the problem related to data, or b) that data protection law could help them in that situation.

When people experience problems in their life that they want to resolve, they will do what they can to deal with that problem. The route to alleviating an issue might include their data protection rights, but they are unlikely to know that. Importantly, they do not think first about their data protection rights and then think about what problems in their life that they could solve with those rights. Rather, they realise they have a problem they want to deal with and then look for ways of dealing with their problem.

Having discussed what our research has indicated about how people understand their data protection rights and where they fit within their everyday lives, we now look at what that means for a) data protection regulators and organisations that support data protection rights, and b) for organisations that collect and use people's personal data.

SECTION 2

Making data protection relevant to people

KEY POINTS

Considering the findings discussed in section one, these are important points to consider when communicating in support of data protection rights:

1. **Provide information and context for data protection rights.** Expect members of the public to require examples of the situations in which they might find data protection rights useful or vital to solving a problem or improving their life in some way. Otherwise, they are unlikely to fully grasp why data protection rights are important. Information about rights is likely to be most relevant at the point when the collection of data is about to start as this is when the context is particularly clear.

2. **Offer services or tools that are problem-focussed rather than rights-focussed.** The implication of the previous point is that services or tools that help people use their data protection rights will likely resonate with more people if it is clear which problems the service helps with. It will likely be more difficult for people to see the benefits of tools which help people use their data protection rights in the abstract.

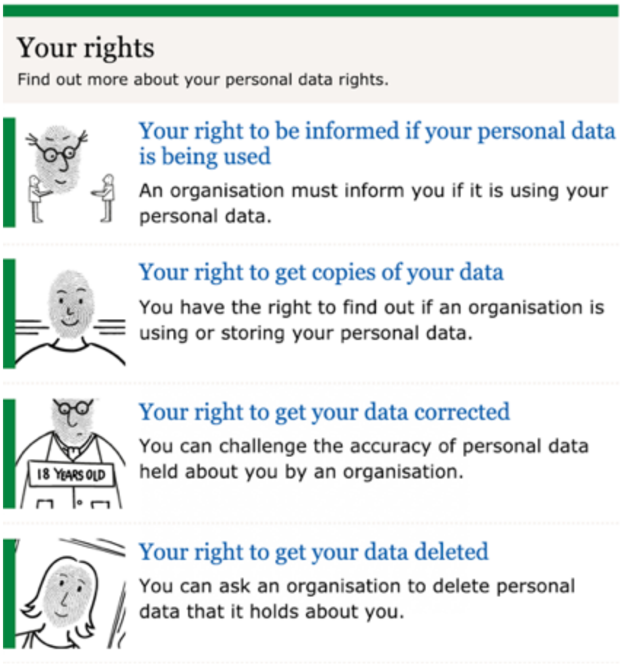
3. **Make time to undertake user-centred research to understand how your target audiences think about data protection and what the problems are in their life.** This will help you tailor your messages for those people and help you show how data protection rights can be helpful to them. Avoid talking to the people you already talk to in your working life about data protection. Test your messages with real people from your audiences, both by talking to them in-person and with technical approaches such as A/B testing.

CONTEXTUALISE AND PROVIDE EXAMPLES OF DATA PROTECTION RIGHTS IN ACTION

Our research suggests that it is rare for members of the public to know about and understand their data protection rights. When people find out about the rights, it is not always immediately obvious to them when the rights would be useful in their daily lives.

The implications of this are that when organisations who support data protection rights communicate about those rights, they must provide real-world examples of when those rights could be useful or vital to people. Otherwise, it is likely that people will not see the immediate relevance of them to their everyday lives or be able to remember that they have those rights when a situation arises where they need them.

A good example of communicating data protection rights themselves and providing added context is the *Your Rights* section of the Information Commissioner's Office *Your Data Matters* pages.[10] While some of the content has very little about why someone might want to use these rights, it goes on to offer specific situations where these rights are relevant.



Your rights

Find out more about your personal data rights.

Your right to be informed if your personal data is being used

An organisation must inform you if it is using your personal data.

Your right to get copies of your data

You have the right to find out if an organisation is using or storing your personal data.

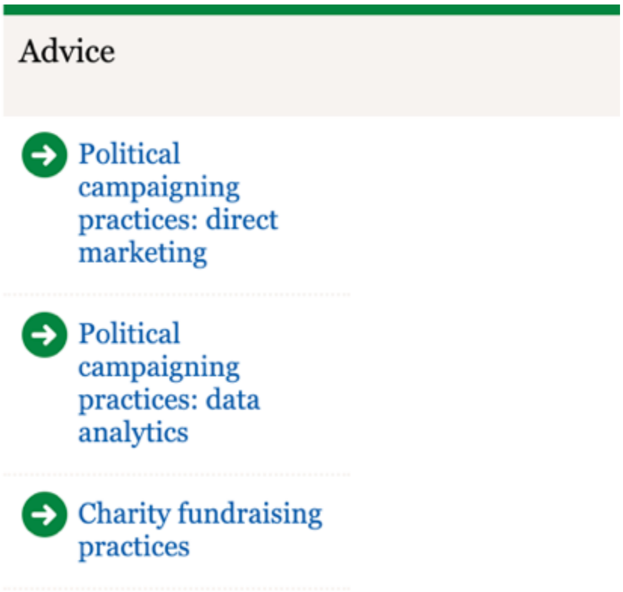
Your right to get your data corrected

You can challenge the accuracy of personal data held about you by an organisation.

Your right to get your data deleted

You can ask an organisation to delete personal data that it holds about you.

A screenshot from ico.org.uk/your-data-matters showing links to information about data protection rights – Ed Johnson-Williams



Advice

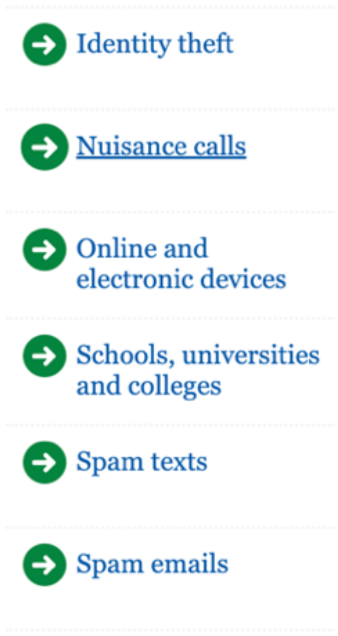
Political campaigning practices: direct marketing

Political campaigning practices: data analytics

Charity fundraising practices

Screenshot 1 from ico.org.uk/your-data-matters showing links to advice about data protection in specific contexts – Ed Johnson-Williams

[10] Information Commissioner‘s Office ,*Your Data Matters* – .https//:ico.org.uk/your-data-matters


Identity theft
Nuisance calls
Online and electronic devices
Schools, universities and colleges
Spam texts
Spam emails

Screenshot 2 from ico.org.uk/your-data-matters showing continued links to advice about data protection in specific contexts – Ed Johnson-Williams

More work is needed to find the best routes of communicating GDPR rights to people to increase awareness and understanding of these rights. Very few people we spoke to during our research were aware of the Information Commissioner's Office, so would be unlikely to visit their website. Communicating the rights is likely to be most successful by going to where people are. Social media, advertising, and press campaigns that highlight real-world problems that data protection rights can help with may be more successful than attracting people to generic information on an institutional website.

Another useful area for future research would be to gather evidence of what the most common situations are where data protection rights could be useful or vital. This would help organisations who want to communicate examples of data protection rights in action by allowing them to highlight the kinds of contexts that a large portion of their audiences would encounter. It would also help creators of tools or services that help people use their data protection rights. They could use this information to make tools that a) are specific to a single context, b) allow a user to select their use-case as a first step, or c) provide examples of situations of when a data protection right is useful in a tool that is rights-focussed.

PROVIDE *PROBLEM-FOCUSSED* TOOLS AND SERVICES

Our understanding from the people we talked to in our various rounds of research is that people do not categorise their life by which data protection rights would be most useful at a given time. Rather, they go about their life and, in some situations, they may look for something that could help them. This appears to be the best opportunity for tools or services that help people use their data protection rights to find their target audience.

Services that deal with specific domains to help people with a particular problem are more likely to align with users' needs and current knowledge than with services that merely present the data protection rights and let the user work out how they can use them. An example of this *problem-focussed* approach, which Open Rights Group is looking to develop, would be a tool to help people with the problem of knowing why an insurance company[11] has set a high quotation when applying for an insurance policy.[12] People often need insurance coverage for their car, house, life, health, dental treatment, travel, public liability, gadgets, pet and so on. If the quotation for that coverage is unaffordable, then it can be a serious problem for the applicant. People could contact the insurance company through a website – built using the public data[13] of company contact details from *Data Rights Finder* – to improve their understanding about how their quotation for insurance coverage had been set.

[11] In practice ,it is often a separate company – an underwriter – that sets the price of insurance .We may have to collect some further contact details data for underwriters that is linked to each insurance company to create this tool.

[12] We had originally thought about making a tool to help people understand why they had been rejected for an insurance policy. In user research to test that idea, it emerged that high and unaffordable prices was a more common problem that was just a serious as not being offered insurance at all.

[13] Data Rights Finder API Documentation – https//:github.com/datarightsfinder/website/blob/master/docs/api.md

The models that insurance companies use to set quotations are likely to include many factors outside of an applicant's knowledge or control. Insurance companies may make their decisions based solely on automated processing, particularly through comparison websites which are a very popular way of applying for insurance. Companies making fully-automated decisions are obliged to provide meaningful information about how they arrive at their decisions and the significance and consequences for the applicant. In this context, that might mean an increased likelihood of having higher quotations in the future.

Understanding the reasons for a quotation being set could help an applicant know that they need to turn to a specialist insurance company or know how to modify their behaviour in the future to improve their chances of being given an affordable quotation. In any event, the data subject should be informed of sources of personal data including public sources such as social media.

This is an approach that helps people with a specific, relatively common, and serious problem. During limited user research, we have found that this is a problem that people recognise and would like help with. There is a good chance that users will quickly understand the value of a service like this and be able to map it onto their everyday lives.

MAKE TIME TO CARRY OUT USER-CENTRED RESEARCH TO UNDERSTAND YOUR AUDIENCE

People told us during our research that the data held in *Data Rights Finder*, such as organisation contact details, how organisations use data, and who they share it with, seemed very useful. People also said, however, that they would be unlikely to see the immediate relevance of the data protection rights presented on the site to their everyday lives.

Our findings highlight the point that helping people access their data protection rights has to be grounded in specific contexts, needs, motivations, and problems. Many organisations and companies are trying to support individuals in engaging data protection rights. We would recommend that time and resources are allocated to carrying out research with potential users – at the beginning and throughout the project – to discover those user needs. We understand that undertaking user-centred research like this might require extra resources, but it can reduce costs and time requirements over the course of a project as well as increasing the likelihood of creating a compelling product.[14]

As discussed in the previous section of this report, Open Rights Group is looking at creating a website that concentrates on the particular problem of the lack of clarity in how insurance coverage quotations are set. To arrive at this problem, we spoke first with a group of experts in finance, debt assistance, and banking regulation to find an area where people experience difficulties relating to finance and data. One person in the group talked about the problem of being rejected for insurance coverage and not being told why. We then spoke with a small number of people in one-to-one interviews to explore their experiences of applying for insurance and of automated decision-making. During that round of research, it became clear that, although the people we spoke to were not rejected for insurance coverage very often, they were confused about how the prices were set and why they were sometimes very high. Although we expect further research to be required to test this idea, this was a better user need on which to focus a digital tool that helped people tackle a real-world problem and that used their data protection rights – to be informed about an automated decision in this case.

This is a short example that shows why much more work is needed to create services and messages about data protection that stand a greater chance of resonating with and making sense to the public.

[14] U.S .Dept .of Health and Human Services ,*Benefits of User-Centered Design* – .https//:www.usability.gov/what-and-why/benefits-of-ucd.html

SECTION 3

How organisations can communicate well about data protection rights

KEY POINTS

From our experience of analysing organisations' privacy policies to create *Data Rights Finder*, talking to people about data protection issues, and carrying out desk research, Open Rights Group has the following recommendations on how organisations can communicate better about data protection:

1. **Provide electronic means such as an email address or contact form to contact your data protection officer.** We found several well-known companies who only provided a postal address as the route through which to use a data protection right. Ideally, all organisations would provide an email address to help people use their data protection rights. As a bare minimum though, companies which do business online should provide electronic means to contact them.

2. **Explain how the data protection rights interact with the particular activities or business that your organisation does.** Help the individuals involved to know what their rights are, how those rights are relevant to their relationship with your organisation, and finally, how and why individuals would use those rights.

3. **Use plain English to describe how you use data.** Tell people clearly what data you collect and what you will use it for. Guidance with examples of good and bad practice and recommended writing styles is available. Test how easy it is to find, read, and comprehend the information you provide about how you use data.

4. **As much as possible, use a granular, rather than a bundled, approach to gaining consent to collect and process personal data.** It is not always reasonable to expect people to give consent to everything in your privacy policy at the very beginning of their relationship with you. Just-in-time information and consent is one way to address this.

5. **Link the data you say you collect with the purpose you will use it for.** When we read privacy policies, we found that organisations often included one list of the types of data they collect and a separate list of the purposes they may use data for. It was very unclear as to which data was being used for which purpose.

6. **Consider alternatives to the name 'privacy policy'.** There is research in America, discussed below, that consistently finds that people misunderstand what is meant by the name 'privacy policy'. Most people assume that when they see that an organisation has a 'privacy policy', it means their information is kept private. In reality, they are documents that explain how an organisation will use information. Phrases like "How we use data" may offer a better alternative.

7. **Contribute to and run trials of machine-readable standards about how you use data.** The way organisations are presenting information about how they use data is inconsistent and unstructured. This makes it difficult for users to find information and to compare it with how other organisations use data. It also increases the challenge to researchers and service designers who want to scrutinise and provide insight into how organisations use data. Organisations should collaborate on and test machine-readable standards to communicate how they use data to help with these issues.

PROVIDING ELECTRONIC MEANS TO USE DATA PROTECTION RIGHTS

Several of the companies whose privacy policies we analysed for *Data Rights Finder* did not provide an email address or contact form to contact their data protection officer. In these cases, the only way to make a request which uses a data protection right is to send a message by post. This is a dark pattern[15] that appears intended to dissuade people from using their data protection rights.

An example of a company that uses this dark pattern is *U K Insurance.*[16] *U K Insurance* is better known by its brand names: *Churchill*, *Direct Line*, *Privilege* and *Green Flag*. The only way that their privacy policy gives to contact them to exercise data protection rights is a postal address.

As part of this research project, Open Rights Group started an application for contents insurance through *Direct Line*. We applied for the coverage on *Direct Line*'s website and received a quotation by email. We replied to the email that included the quotation to request an explanation of how the automated process had arrived at the quotation. The logic involved had not been communicated to us during the application process. We also made a phone call to *Direct Line*'s customer service line to ask for an explanation and for electronic contact details for *U K Insurance*'s data protection office. The customer advisor did not know that information. We were put on hold for ten minutes and then disconnected. At the time of this report's publication, we have been waiting for a reply to our request for over a month. In that time, we have, however, received two (automated) requests for feedback by email.

Ideally, all organisations would provide an email address to help people contact them to make a request using their data protection rights. In the case of companies such as *U K Insurance* that do their business online, not offering electronic means for their customers to use their data protection rights appears to be a manipulative attempt to dissuade people from using their data protection rights.

EXPLAINING HOW DATA PROTECTION RIGHTS WORK IN CONTEXT

In our privacy policy analysis for *Data Rights Finder*, we found that many organisations are almost copy-pasting the rights from GDPR into their privacy policy. This is not working as an approach to building awareness or understanding. It is important to explain

[15] Dark patterns are deceptive user experience or user interface designs that aim to manipulate or mislead users or to make them do something that they do not want to do .This is a good introduction to dark patterns :Arushi Jaiswal ,*Dark patterns in UX :how designers should be responsible for their actions* – .https//:uxdesign.cc/dark-patterns-in-ux-design7009-a83b233c

[16] There is a space between the' U 'and the' K 'of *U K Insurance*.

how these rights interact with the particular activities or business that the organisation does and make it clear how this affects the individuals involved.

As an example of the kind of practice we have seen, Coinbase UK – a digital currency wallet and exchange – starts describing GDPR data protection rights 5,023 words into a 6,252 word privacy policy. Below is a quotation from the Coinbase privacy policy to illustrate how the rights are being communicated and the kind of language being used.

> **Right to erasure.** You have the right to request erasure of your personal information that: (a) is no longer necessary in relation to the purposes for which it was collected or otherwise processed; (b) was collected in relation to processing that you previously consented, but later withdraw such consent; or (c) was collected in relation to processing activities to which you object, and there are no overriding legitimate grounds for our processing. If we have made your personal information public and are obliged to erase the personal information, we will, taking account of available technology and the cost of implementation, take reasonable steps, including technical measures, to inform other parties that are processing your personal information that you have requested the erasure of any links to, or copy or replication of your personal information. The above is subject to limitations by relevant data protection laws.

An example from coinbase.com/legal/privacy of data protection rights being communicated

This text appears to be generic. We very quickly found many examples of identical text in the privacy policies of other companies.[17] We expect very few people to be able to find this information, to understand it, to be able to use it, or to know why they would use it.

This is not to make an example of Coinbase. Coinbase is not unusual in this regard. However, we have established in our research that people do not understand their data protection rights without context. Repeating the text of GDPR is not helping people to understand how an organisation uses data. It is important to explain how these rights interact with the particular activities or business that the organisation does and make it clear how this affects the individuals involved.

COMMUNICATING HOW DATA IS USED IN "CLEAR AND PLAIN LANGUAGE"

It is important to be clear with people about what data is collected about them and what it will be used for. Being transparent helps to build trust and accountability about how data is used.

Article 12.1 of GDPR says that organisations that process data should provide information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child." To help organisations do that, the Article 29 Data Protection Working Party (WP29)[18] – a body made up of representatives from the data protection authorities in each EU member state – has published comprehensive guidance on transparency around processing of personal data under GDPR.[19]

[17] Send Pilot, *Privacy & GDPR* – https://www.sendpilot.co/privacy; Cities Foundation, *Privacy* – https://citiesfoundation.org/privacy; CastleCoin, *Privacy Policy* – https://castlecoin.io/privacy-policy-2; Bitqist, *Privacy Policy* – https://support.bitqist.com/hc/en-us/articles/360002266632-Privacy-Policy; Le Agency, *Privacy policy* – https://leagency.com/privacy-policy

[18] This is now replaced by the European Data Protection Board.

[19] Article 29 Newsroom, *Guidelines on Transparency under Regulation 2016/679.* – https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

POOR PRACTICE EXAMPLES

The following phrases are not sufficiently clear as to the purposes of processing:

- ***"We may use your personal data to develop new services."***
  (It is unclear what the "services" are or how the data will help develop them.)
- ***"We may use your personal data for research purposes."***
  (It is unclear what kind of "research" this refers to.)
- ***"We may use your personal data to offer personalised services."***
  (It is unclear what the "personalisation" entails.)

GOOD PRACTICE EXAMPLES

- ***"We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in."***
  (It is clear that what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this.)
- ***"We will retain and evaluate information on your recent visits to our website and how you move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive."***
  (It is clear what type of data will be processed and the type of analysis which the controller is going to undertake.)
- ***"We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read."***
  (It is clear what the personalisation entails and how the interests attributed to the data subject have been identified.)

Examples of clear and plain language as given by the Article 29 Data Protection Working Group

According to the WP29 guidance,[20] being concise and transparent means communicating "efficiently and succinctly", allowing users to quickly navigate to a specific section rather than scrolling through large blocks of text, and separating privacy-related information from terms of use. Organisations should ensure that people are able to understand "the scope and consequences of the processing" and will not "be taken by surprise at a later point about the ways in which their personal data has been used." Privacy policies being intelligible means they "should be understood by an average member of the intended audience." To be easily accessible, it should be "immediately apparent…where and how this [privacy-related] information can be accessed." Finally, to use clear and plain language, organisations should provide information in "concrete and definitive" language while avoiding "abstract or ambivalent terms",

[20] See pages 7-10 of the WP29 guidance for further information in this area.

"complex sentence and language structures" and "overly legalistic, technical or specialist language or terminology."

The WP29 guidance gives examples of good and bad practice in this area. They are particularly useful to understand what the requirements are so we are reproducing them from WP29's guidance here with very light editing of line-spacing to improve readability.[21]

As well as following the WP29 guidance, it is also a good idea for organisations to carry out usability and readability testing of their privacy-related information. This would look to answer questions including:

- ***Can users find this information within the user interface of the website or product?***
- ***Can users find information within the privacy policy?***
- ***Can users understand the information in the privacy policy?***
- ***When users sign up for a service, how well do they understand what data will be collected and how it will be used?***

These questions could be addressed in usability testing with real users.

Another area to consider is how comprehensible the text of the privacy policy is to an organisation's users. One common way of assessing this is with a cloze test where every sixth word is replaced by a blank space and people try to guess the missing words. If the average score is above 60%, that usually indicates that the text is comprehensible to an organisation's users, assuming the participants are roughly representative of those users.

Recent research in America looked at people's preferences when online behavioural advertisers communicate about why an advert is being shown. They found that people preferred explanations which included specific and personalised information about why an advert was presented to them. They also found that "vague and oversimplified language made many existing ad explanations uninterpretable and sometimes untrustworthy." Many organisations could benefit from carrying out similar research to understand how their users would prefer to be told about how data about them is being used.

ASKING FOR CONSENT USING GRANULAR, NOT BUNDLED, APPROACHES

When organisations are relying on an individual's consent to process data about them, they are commonly asking the individual to consent to all the processing, all at once. This can be an overwhelming experience for individuals. As mentioned above, most people do not have the time or energy to assess whether they are happy for their personal data to be processed for all the reasons given in a privacy policy. So-called 'just-in-time' design patterns that allow organisations to ask for consent and provide information at the specific time a user is about to carry out a task may offer a useful way forward. This is less burdensome on the individual and still allows an organisation to rely on consent to process personal data.

Many organisations bundle privacy policies into general Terms and Conditions that users are required to agree to in order to use the service. In many cases, the processing of personal information will not be based on consent, but users could be easily confused between the acceptance of general Terms and consent for data processing. In cases where the processing is not based on consent, people still need to be informed. There might be value in developing a design pattern that separated out collecting consent from collecting confirmation that the user has read the information about processing.

[21] See page 9 of the WP29 guidance for the original of this.

WE COLLECT:

Your email address

WHY WE COLLECT IT AND HOW WE USE IT:

- ***To create and support your account and provide you with Services.***
- ***To communicate with you, for example, informing you about your account status, security updates and website and mobile application information.***
- ***To contact you about features, products, services and other promotions that can enhance your use of the Services, in accordance with your communications preferences.***
- ***To enforce compliance with our Terms.***

HOW WE RETAIN IT:

We keep your email address until you delete your account by sending an email to support@aisense.com

An example from otter.ai/privacy of a structure that links category of data very closely with purpose of processing

BEING CLEAR ABOUT WHAT DATA WILL BE USED FOR EACH PURPOSE

It is very helpful when organisations structure their privacy policy in a way that tightly links together data that they collect with how it will be used. We found many examples where this was not the case. Privacy policies often list the data that is collected and then separately list the purposes that data could be used for. It is very unclear though which data is used for which purpose.

Otter.ai is an example of a privacy policy that is structured in a helpful way. They state a single category of data that they collect, e.g. email address. They then say why they collect a user's email address and how they use it. Finally, they say how long they retain the email address. It repeats this structure for every category of data they collect.

Unless a structure along these lines is kept to, it can be very difficult to work out why certain pieces of data are being collected. This can lead to a lack of trust in the organisation. It is confusing, for example, when a financial organisation says in their privacy policy that they collect data on your phone's battery level. It is not clear why that is happening. It could be to create data about how risky your behaviour is: 'Does this user leave their house with low phone battery on a consistent basis?' On the other hand, the data could be collected to ensure that the organisation's phone app does not overtly drain the user's phone battery. One of these uses for the data has the potential to be more privacy-invasive than the other. Unless purposes are clearly linked to the category of data, users will find privacy policies unclear and will not be able to fully understand how their data is going to be used.

CONSIDERING WHETHER ‘PRIVACY POLICY’ IS THE BEST LABEL FOR PRIVACY-RELATED INFORMATION

The vast majority of organisations that we have seen refer to the document containing information about how they use data as a ‘privacy policy’ or a ‘privacy notice’. The label of ‘privacy policy’ may, however, be widely misunderstood.

Research carried out in America[22] has consistently found over fifteen years that when people see an organisation has a privacy policy, they assume that means their data will be kept private and secure.[23] This is not necessarily true. In fact, the privacy policy documents themselves often reveal data practices that appear privacy-invasive. It is possible that the findings of this research would be replicated if carried out in the UK.

Given this, it would be worthwhile for organisations to consider whether the label ‘privacy policy’ or ‘privacy notice’ is the best name. Examples of names that organisations have used instead of ‘privacy policy’ include *“How we use your information”* (Accent Housing)[24], *“How IF uses data”* (Projects by IF)[25], and *“How We Use and Protect Your Data”* (Privacy International).[26] Other UK-based organisations, particularly in the public sector, often use the term ‘fair processing notice’. Research into whether people in the UK understand the term ‘privacy policy’ should also look at whether people understand ‘fair processing notice’. It seems unlikely that they will considering the findings of our research.

CONTRIBUTING TO MACHINE-READABLE STANDARDS ABOUT HOW ORGANISATIONS USE DATA

We have looked at a lot of privacy policies during this project and found that information about how organisations use data is often presented in an inconsistent and unstructured way. This means users will find it hard to discover the information and to compare various organisations’ use of data. There is also a community of researchers and service designers who want to examine how organisations use data and to make tools which help individuals understand how their data is processed or to use their data protection rights.

The data in *Data Rights Finder* was manually drawn together because privacy policies are presented in a way that is not structured or consistent enough to allow more automated collection of the information.[27] We have seen privacy policies presented as PDFs, multiple webpages, and single webpages. The location of the privacy policy within websites is not consistent: both in terms of the URL and where to find a link to it in the user interface. Privacy policies often use different phrases for the same thing – both within the same organisation and between different organisations. An example of this would be saying “How long do we keep your data for?” versus “Retention period”, or “Location data” versus “We monitor where you take your phone”. To try to overcome these issues, we developed a data structure to capture the various ways in which organisations use and refer to data.[28]

[22] Joseph Turow, Michael Hennessy & Nora Draper, *Persistent Misperceptions: Americans’ Misplaced Confidence in Privacy Policies, 2003–2015.* – https://www.tandfonline.com/doi/full/10.1080/08838151.2018.1451867
The journal article about this is behind a paywall. The author wrote an op-ed in the *New York Times* that makes the same argument and is not behind a paywall: Joseph Turow, *Let’s Retire the Phrase ‘Privacy Policy’*. – https://www.nytimes.com/2018/08/20/opinion/20Turow.html

[23] One interesting aspect of the research that is not directly relevant to this report was that people who correctly understood what the “privacy policy” label means were likely to believe that that privacy laws needed to be stronger. People who did not correctly understand “privacy policy” were likely to see no need for changes in laws governing privacy.

[24] Accent Group, *Your Information*. – https://www.accentgroup.org/how-we-use-your-information

[25] Projects by IF, *How IF uses data*. – https://www.projectsbyif.com/how-if-uses-data

[26] Privacy International, *How We Use and Protect Your Data*. – https://www.privacyinternational.org/basic-page/618/how-we-use-and-protect-your-data

[27] There is one project we are aware of that attempts to use machine learning to analyse privacy policies: Pribot, *AI-Powered Privacy Policies*. – https://pribot.org

[28] Data Rights Finder, *Data* – https://github.com/datarightsfinder/data

Cliqz – a company that makes browser extensions to reduce the effectiveness of web trackers – has made recommendations for four machine-readable standards for communicating how an organisation uses data.[29] We do not necessarily think all of these recommendations are the best answer to the above problems, but they are a useful intervention in this area.

The first recommendation is for a text file containing the privacy policy to always be available at 'example.com/privacy-policy.txt'. This would mean researchers could always rely on finding a privacy policy in the same place. The second was for a "structured list of third parties", "the service being performed by them", and a "list of data points they have access to" to be available at 'example.com/third-parties.json'. Cliqz appears to be focussing here on websites, but this could be repurposed for organisations as a whole. The third idea was for some structured contact data for the Data Protection Officer at an organisation to be made available at 'example.com/dpo.json'. This would allow services to build tools to help people use their data protection rights. The final suggestion was for structured data about data incidents to be kept at 'example.com/incidents-and-cases.json'. The intention is that this would improve transparency about whether there had been data breaches and so on.

Another approach to such a standard would be for organisations to include a link to their privacy policy in the HTML head of every webpage. This would be most effective if the link included a standard 'rel' attribute to ease automated discovery. This is an example of what that might look like:

**<link rel=”personal-data-usage”
href=”https://organisationname.com/
whereever-their-privacy-policy-is”>**

This approach could be combined with a standard, agreed-upon scheme of HTML markup (probably classes or IDs) which would label specific sections of a privacy policy such as contact details, types of data collected and so on. This could ease the burden of adopting open standards in this area on organisations and would allow them to provide machine-readable signposts to where their privacy policy is and the information within it without needing to create a new webpage or structured data file.

We would like to see further investigation into what standards around structured data about how organisations use data would be most useful for individuals, researchers, service designers and others. It would be important to understand the drivers of adoption of other similar standards such as 'robot.txt'[30] and 'ads.txt'[31] and to build support for the standard among organisations themselves. In the future, we would like to be able to integrate structured data created by organisations into *Data Rights Finder* in an automated way.

[29] WhoTracks.me, *GDPR - What happened?* – https://whotracks.me/blog/gdpr-what-happened.html#recommendations-for-gdpr-20

[30] The Web Robot Pages, *About /robots.txt* – http://www.robotstxt.org/robotstxt.html

[31] IAB Tech Lab, *About ads.txt* – https://iabtechlab.com/ads-txt-about

ico.
Information Commissioner's Office

Grant Recipient

We are grateful to the Information Commissioner's Office (ICO) for funding this research through their Research Grants Programme.