Data protection rights: What the public want and what the public want from Data Protection Authorities

Executive Summary

1. In order to be effective Data Protection Authorities (DPAs) need to understand what the public are concerned about, how they understand their data protection rights, what they expect DPAs to do to uphold their rights and how they would like to be empowered by DPAs to use them.

2. There is of course no 'one size fits all' view on what the public are concerned about, at more granular level there are much more nuanced views on sharing their personal data and how this should be used by organisations and what they would like to see from DPAs. There are however a number of themes which appear from the views of the public across Europe.

3. The commonly recurring themes of what the public want from data protection are;

    - Control over their personal data;
    - Transparency – they want to know what organisations will do with their personal data;
    - To understand the different purposes and benefits of data sharing;
    - Security of their personal data; and
    - Specific rights of access, deletion and portable personal data.

4. The themes of what the public want from DPAs are;

    - Independence – DPAs free from outside influence;
    - Consistency – where possible a consistent approach to data protection across the EU;
    - Visibility – DPAs making themselves known, providing clear help and guidance to them and also to organisations;
    - Privacy certification, seals and trust marks – giving them confidence in the organisations who are processing their personal data;
    - Responsive to new technologies – DPAs that understand the privacy implications of the new technologies they encounter in their daily lives; and
    - Enforcement – appropriate remedies that are used effectively by DPAs to ensure that organisations comply with data protection rules.

5. DPAs need to get practical and creative in their response to what the public want – to get the most out of often limited budgets alongside rising numbers of complaints and new data protection challenges driven by technology.

Introduction

6. UK and EU research reveals that concerns about privacy and the protection of personal data are increasingly of importance to the public. A perceived lack of control over their data along with high profile losses of personal data by organisations add to the feelings of concern. Yet we are all creating more information about ourselves and making this more widely available than ever before – everything from social networking to sharing data from fitness apps. There is a real negative-positive tension here and it is the role of Data Protection Authorities (DPAs) to manage this so that – as far as is possible – the public get the best of both worlds; privacy and control but also access to the services and experiences they increasingly rely on, enjoy and take for granted in today's information society.

7. The public need to be empowered by DPAs to understand what their rights are, how to use them and what they should expect from organisations. Likewise the public rely on DPAs to ensure that organisations are aware of their obligations, and to take enforcement action where necessary to ensure compliance and to act as a wider deterrent. They also want help from DPAs – they want their specific, individual, data protection concerns resolved – something that is becoming increasingly difficult to deliver given the sheer scale of

personal data processing and increasing public awareness of information rights issues.

8. The importance of privacy on the public's agenda is a complex issue. Whilst in surveys and research the public generally state that they are concerned about how and why their personal data is being processed this is often in contrast to how the public actually behave in their daily lives.

9. As more of the public's daily lives are spent online and the range information held about them by organisations increases and is more likely to be processed electronically, this brings in new challenges for DPAs. The purpose of this paper – and this conference – is to determine what those challenges are and how best to deliver what the public wants from us.

10. This paper has been produced by the Information Commissioner, the UK's Data Protection Authority and draws together common themes from recent pan European research, along with research conducted in the UK and the Commissioner's own experience of these themes. To supplement the findings from the secondary research the Information Commissioner also commissioned some focus groups made up of members of the public to understand their views on privacy and data security specifically in relation to use of the internet.

11. The purpose of this paper is to provoke discussion and debate. We want to know what the public wants from us and how we can best deliver that. For ease of reference, specific points for discussion have been highlighted by blue boxes.

What do the public want?

12. Understanding what the public want from data protection is key. However the views of the public can appear to be contradictory - with what they say they want often not mirroring their behaviour. Likewise the public's attitudes towards data protection and their personal data are hard to characterise as one common view. Research in the UK by Citizen's Advice[1] (a service which provides advice to the public on a variety of topics) found that privacy is a personal setting with only the individual knowing what they are comfortable sharing and on what basis.

[1] Citizens Advice – Personal data empowerment Time for a fairer data deal? (April 2015) https://www.citizensadvice.org.uk/Global/CitizensAdvice/Corporate%20content/Publications/Personal%20data%20empowerment%20report.pdf

13. The public can be given any number of rights and protections however if the public find these confusing or burdensome, or indeed unhelpful, then we have failed in our mission to provide the services and mechanisms to help educate and empower the public and to help uphold these rights.

14. The public also expect DPAs to take action when data protection laws are seriously contravened and take proactive steps to ensure organisations get compliance 'right first time'.

15. Both the public and organisations have a range of expectations about what a data protection regulatory system should be able to deliver – it is impossible and unrealistic to meet all of these. A balance must be struck between ensuring the public have access to the correct tools to enable them to assert their rights but ensuring that organisations make these work in practice.

Control over their personal data

16. A common theme appearing in research into the public's views, both Europe wide and in the UK is one of control. The public are often uncomfortable with providing their personal data to organisations as they perceive that once it has been given they lose control of it.

17. Consent will always be a key condition in data protection legislation but it is becoming increasingly important to consider consent within the concept of control.

18. Eurobarometer research[2] found that 74% those surveyed see having to disclose personal data as an increasing part of modern life. Research by Sciencewise (a UK Government funded programme)[3] concluded that although the public are aware that they need to disclose their personal data as part of their day to day life, there is concern about losing control of their that data and the public are keen to have more control over how it is used.

19. Recent research in the UK by the ICO[4] found that when the public were asked to what extent they agreed or disagreed that '*you have*

[2] Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
[3] Sciencewise - Big Data, Public views on the collection, sharing and use of personal data by government and companies (April 2014) http://www.sciencewise-erc.org.uk/cms/assets/Uploads/SocialIntelligenceBigData.pdf
[4] Information Commissioner's Office - Annual Track individuals (September 2014) https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf

lost control over the way your information is collected and processed' 63% agreed with this statement. The research also found that 85% of respondents were concerned about organisations passing or selling their personal details onto other organisations.

20. The public's control issues are compounded by worries they have such as inaccurate data held by one organisation which then gets shared with other organisations, making correction of the data difficult. DPAs have a role to play by ensuring that they are able to step in and protect the rights of the public where these worries become a reality.

21. The public however appear to have developed their own methods of dealing with their perceived lack of control over their personal data. One way that individuals try to retain control is to avoid providing personal data and Eurobarometer research has shown that in order to protect their identity over half of the public will only provide organisations with the minimum amount of information required to access the service/goods[5].

22. Likewise research from Symantec[6] found that 57% of the public in the seven European countries surveyed are now avoiding posting their personal details online. This corresponds with the findings of the Eurobarometer 'Cyber Security' research[7] in which 89% of respondents agreed that they avoid disclosing their personal information online. The Symantec research also found that 33% of respondents admitted to providing false details online in order to protect their privacy.

23. Avoiding providing personal data online and providing false details means that organisations (both private and public) are missing out on potential customers and the data which they are collecting and basing decisions on may be of little value.

24. Recent focus group research conducted on behalf of the ICO[8] found that whilst the public take precautionary action providing personal data online, convenience often outweighs the perceived risks. Likewise although there is a general feeling of mistrust in the online environment the public will continue to use online services seeing the potential problems as being a 'necessary evil'.

---

[5] Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) '62% of Europeans give the minimum required information' http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[6] Symantec - State of Privacy Report 2015 (February 2015) http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf

[7] Special Eurobarometer 423 – Cyber security (February 2015) http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

[8] ICO - Consumer attitudes to privacy and data protection (April 2015)

25. The question, though, is what are appropriate degrees of control? And what control mechanisms are effective? Whilst the public clearly fears losing control of their personal data how much control do they actually want? For example websites now must display information about cookies and consent, to comply with Directive 2002/58/EC, which in theory puts the public in control. There has been much debate and discussion about a 'do not track' solution at browser level, but effective browser based solutions have not emerged. It is unclear to what extent the mechanisms currently used are delivering real control for the public – more research is needed in this area.

26. Clear unambiguous opt-ins and default settings are one way of ensuring the public feels in control rather than the current situation where organisations often use a confusing array of opt-outs and opt-ins which are sometimes pre-ticked and sometimes the accompanying text written with a double negative seemingly designed to deliberately confuse the public.

27. Currently once the public have opted in, or indeed forgotten to opt-out, their personal data is often sold on to other companies several times over seemingly for an indefinite timescale. DPAs should ensure that they are taking action to tackle contraventions that occur as a result of such practices. However, we have to do more to understand the choices and information the public want in these situations. Choices need to be far clearer and easy to understand, with default options that always allow the public to protect the use of their data. More could be done to develop standardised symbols that convey information about proposed processing.

28. Little is still known about what the public may engage with - it may be that some groups of the public 'want their cut' when their personal data is being 'monetised' by those they entrust it to. This isn't really about privacy – perhaps it is more about equity and fairness in a mainstream consumer rights sense.

29. In the ICO's focus group research the public were aware of the control settings which social media sites provide and the importance of these settings. However the settings were seen as confusing and time consuming to use as the sites often changed how the settings work.

30. It seems increasingly likely that in the future there will be technical solutions available to the public to control how their data is shared online. For example a recent UK media article[9] referred to research by computer scientists at Queen Mary University of London and

[9] The Guardian (1 February 2015) http://www.theguardian.com/technology/2015/feb/01/control-personal-data-databox-end-user-agreement

Cambridge University into computer software which an individual would use to collect their personal data from their devices and make it available only to those organisations which the individual allowed. There are already some technical solutions available, for example the company Ghostery provides privacy tools[10] which allow the public to see which companies are tracking them online and enables these trackers to be blocked.

31. These solutions may work well for certain groups of the public but solutions must be developed to meet the range of levels of digital literacy the public have. Equally, the better the levels of digital literacy the public have, the more reasonable it is to promote these solutions.

32. It is important that DPAs are able to keep pace with such potential technological advances and we will consider this later in this paper.

33. Control issues are multi-stranded and manifest into different areas such as transparency, individuals rights and the security of personal data. It does seem clear that services such as social networking are 'teaching' the public to make increasingly sophisticated choices over who has access to particular bits of information about them. Some sections of the public are becoming more used to managing multiple identities and controlling their privacy in a real-time, active way that was unheard of just a couple of decades ago. We expect this tendency to continue. DPAs need to understand how this process can evolve and how they can intervene to ensure it becomes a 'race to the top', for example in default settings. Learning about control also needs to be part of the digital literacy agenda.

The challenge for DPAs is to strike the right balance in identifying the areas where promoting the concept of control is most useful in enabling the public's data protection rights and assessing whether organisations can deliver in practice. Is there more DPAs can do to explain and share good practice in relation to control mechanisms?

Transparency

34. Organisations should be ensuring that they are transparent with the public about the purposes that they intend to process personal data and who it might be disclosed to. In practice however there is a general lack of trust from the public that organisations will do what they say they will.

[10] https://www.ghostery.com/en-GB/home

35. The public's concern over the control of their personal data is often because they are worried as to what will happen to their personal data and what it will subsequently be used for. Eurobarometer research[11] found that 70% of respondents were concerned that their personal data held by organisations may be used for a purpose other than that for which it was collected. The research concluded that the potential misuse of personal information may be one explanation of the general distrust Europeans have in commercial companies to protect their data.

36. It is clear that the public value the data minimisation principle and want only the minimum amount of personal data to be collected for the organisation's particular purpose or purposes and are concerned that they are being asked to provide too much unnecessary personal data.

37. Is it the case that the public are not being told clearly why the collection of certain personal data is necessary? Or could it be that organisations are trying to obtain information which is simply unnecessary for their purposes?

38. Research by Sciencewise[12] found that awareness of data collection and use by government and companies is quite high, but the level of understanding of what this means in practice is much lower. The research also found that there is strong support from the public for more information on how organisations collect, share and use data.

39. Often privacy notices/terms and conditions are vast documents containing legal language which can be difficult and confusing for the public to understand. In the Symantec research[13] 59% of respondents said that they only skim read the terms and conditions when buying products or services online and 14% said they never read the terms and conditions.

40. The Eurobarometer research found that 58% of respondents who use the internet usually read privacy statements. However 24% of those who read them said that they did not fully understand what they are reading. Those respondents who usually did not read privacy statements on the internet were asked why they did not do so and the research found that 41% felt it was sufficient for them to simply see that websites have a privacy policy, 27% believed that the law

[11] Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
[12] Sciencewise - Big Data, Public views on the collection, sharing and use of personal data by government and companies (April 2014) http://www.sciencewise-erc.org.uk/cms/assets/Uploads/SocialIntelligenceBigData.pdf
[13] Symantec - State of Privacy Report 2015 (February 2015) http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf

would protect them in any case and 24% thought that the websites would not honour the privacy policy anyway.

41. In the ICO focus group research[14] awareness of privacy notices was extremely limited and at best the term itself was recognised and a minority guessed that they were designed to explain how data is protected, not to share personal data or use for further purposes.

42. Often, even if the public do not understand the privacy implications of providing their personal data to an organisation they will still provide it if they want the product/service. The Sciencewise research confirmed that there was a significant discrepancy between the public's stated preferences in regard to collection, sharing and use of their personal data by organisations (generally one of opposition) and their actual behaviour. The discrepancy was in found in part due to the public not having the information required to rationally make decisions about their personal data on a day to day basis; therefore the public may find their general concerns are over-ridden by their more immediate interests. The research concluded that this suggests that implied consent is not a reliable indicator of actual consent, but neither necessarily is stated preference.

43. UK Citizens Advice research[15] found that the public are generally given a blanket either/or choice when it comes to accessing a product or service as there is no opportunity to agree to some parts but not others of a privacy notice. Given that privacy issues were found to be a personal setting this means that effective public control is minimised by privacy notices which establish a blanket permission that covers every eventuality and allow everything.

44. The importance of granular choices when consenting to marketing was highlighted in a recent ICO investigation[16] into UCAS (a UK organisation through which applications are processed for entry to higher education). The application form used by UCAS only allowed applicants to opt-out of receiving marketing from commercial companies if they un-ticked three boxes covering marketing emails, post and text messages. However the wording of the opt-out also meant that un-ticking these boxes would result in the applicant not receiving information about career opportunities and education providers or health information. The ICO ruled that this approach meant applicants felt obliged to let UCAS use their information for

[14] ICO - Consumer attitudes to privacy and data protection (April 2015)
[15] Citizens Advice – Personal data empowerment Time for a fairer data deal? (April 2015) https://www.citizensadvice.org.uk/Global/CitizensAdvice/Corporate%20content/Publications/Personal%20data%20empowerment%20report.pdf
[16] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/04/ucas-application-form-to-be-changed-following-ico-concerns-over-marketing-practices/

commercial purposes otherwise they would potentially miss out on important information about their career or education.

45. There are a number of ways in which DPAs could encourage greater transparency such as layered privacy notices which for example at the start have a list of the key points in easy to understand language which then goes on to use the legal language should the public wish to read more detail. Or there could be more technical solutions to explaining to the public what happens to their personal data for example explaining behavioural advertising using a series of diagrams and pictures. It may be that encouraging organisations to use privacy notices which provide the public with choices so that it can be more tailored towards an individual's personal views on their privacy is the way forward.

46. 'Just in time' methods can give the public clear choices at significant points in their 'informational journeys'. There is a case for considering privacy as more of an activity and less a matter of 'being told something' in a long terms and conditions-type privacy notice that very few people read.

There is a question as to whether DPAs should take a more proactive role scrutinising privacy notices for unfair terms so that the public doesn't have to? Mechanisms such as privacy seals (covered later) can also play a role.

Understanding the different purposes and benefits of data sharing

47. The sharing of personal data is becoming increasingly common in organisations (both private and public) driven by concepts such as 'big data'[17]. The public however are becoming more uneasy with the apparently routine sharing of their information especially where this does not have any tangible benefit to them or the purpose is unclear.

48. The Sciencewise research[18] surmised that personal benefit is the strongest incentive for being in favour of the collection and use of personal data however the public reported that they were currently seeing little benefit from sharing their data and lacked confidence that they will see any benefits in future.

[17] ICO – Big data and data protection (28 July 2014) https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf

[18] Sciencewise – Big Data; Public views on the collection, sharing and use of personal data by government and companies (April 2014) http://www.sciencewise-erc.org.uk/cms/assets/Uploads/SocialIntelligenceBigData.pdf

49. A similar view came from the Symantec research[19] as 81% of those surveyed thought that their personal data has a value and 74% thought it is unfair that companies are making money from their personal data.

50. This is not to say that the public necessarily wish to make money from the sharing of their personal data or that the benefits of data sharing must be on a personal level (eg a better tailored service or discounted goods). The Sciencewise research observed that the public also consider wider societal benefits as a reason why they would find the sharing of their data more acceptable (eg health research, crime prevention etc).

51. Research in Scotland into public acceptability of data sharing[20] found that there was near universal acceptance of public bodies having access to data and there was a commonly held view that public sector organisations were concerned with delivering public benefits or promoting 'public good'.

52. Private sector involvement in data sharing was more contentious and there was strong opposition to data being used by the private sector for the sole purpose of profit maximisation. However respondents were not completely opposed to the private sector accessing data and the view was that access to personal data should only be granted where this is likely to result in some form of public benefit and that their access to data should be more strictly controlled.

53. Whilst generally the public view data sharing in the public sector as 'good' and data sharing in the private sector as 'bad' there can also be a more nuanced view depending on the circumstances. For example when the Scottish research presented respondents with specific types of private organisation it found that the majority felt that pharmaceutical companies should be able to access data from other sectors - the general view being that research by these companies contributed towards understanding of diseases and to new treatments, ie there was a benefit to society. However there was still some unease at the scale of the profits that this type of organisation could generate from using such data.

54. A similar pattern was seen in the Sciencewise research with the trade-off between data sharing and privacy being affected by

[19] Symantec - State of Privacy Report 2015 (February 2015) http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf

[20] The Scottish Government – Public Acceptability of Data Sharing Between the Public, Private and Third Sectors for Research Purposes (2013) http://www.gov.scot/Resource/0043/00435458.pdf

differences in the type and format of the data, the proposed use, type of organisation and the possible advantages/disadvantages.

55. Clearly this provides a lesson for organisations as to how they may be able to transparently explain data sharing to the public. There is of course a role for DPAs to ensure that data sharing is being conducted in a transparent, fair way.

DPAs will need to often assess the public interest in data sharing when considering the data protection principles and conditions for processing. There is a question as to how far DPAs should go with this type of assessment and do we have skills and knowledge to properly make these assessments?

Security of their personal data

56. The public's concerns about a lack of control strongly relate to security fears and the fact that they do not trust organisations to keep their personal data secure. There are frequently high profile losses of personal data in specific EU countries and increasingly cross border security issues which affect the public across the EU, for example in 2011 the Sony Computer Entertainment Europe Limited's Sony PlayStation Network Platform was hacked, compromising the personal information of millions of customers[21] leading to a £250,000 fine from the ICO.

57. In Symantec research[22] 57% of respondents were worried that their personal data was not being kept safe by organisations and 88% felt that keeping data safe and secure was a factor of importance when choosing an organisation to shop with or use.

58. With more and more personal data being held electronically the risks to organisations from technological problems and vulnerabilities to outside attack are high. A recent Eurobarometer 'Cyber Security' report[23] found that internet users are more likely to have changed their online behaviour because of security concerns and 73% of the respondents agreed that they are concerned that their online personal information is not kept secure by websites.

[21] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2013/01/sony-fined-250-000-after-millions-of-uk-gamers-details-compromised/
[22] Symantec - State of Privacy Report 2015 (February 2015) http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf
[23] Special Eurobarometer 423 – Cyber security (February 2015) http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

59. A similar picture has arisen in recent UK research[24]. When respondents were asked to what extent they agreed or disagreed that 'online companies collect and keep your personal details in a secure way' only 22% agreed with that statement.

60. Research into the particular organisational sectors which cause the most security concerns for the public can often be influenced depending on whether a high profile loss of personal data has happened recently. For example the research by the Scottish Government[25] found that security and surveillance firms were commonly distrusted, which owed in part to the fact that at the time of the research there had been high profile data protection failures by a security organisation.

61. However there appears to be an exception to this in regard to public sector organisations. The Scottish research found that despite concerns about public officials misplacing or losing data (as there have been a number of high profile UK public sector data losses both at national and local levels) there was still an assumption that public bodies had more stringent data protection and security procedures in place than other types of organisation, or at least were more accountable to the public when a breach occurred than other types of organisation.

62. Whilst research into security of personal data tends to focus on the public's views and how important it is viewed, it is interesting to note that research in the UK in 2013[26] found that only 63% of the organisations surveyed were aware of the obligation to keep personal data secure.

> So how do we ensure that security is taken as seriously by organisations as it is by the public? Is it a case of greater education of organisations, targeting specific sectors of concern, or are greater penalties for security breaches needed? Or how can we best combine these approaches? The public overwhelming want to be informed by both private and public organisations if their personal data is lost or stolen, demonstrated by 87% of respondents to the Eurobarometer[27] research stating this preference. Is there more we can do to ensure that this happens?

[24] Information Commissioner's Office - Annual Track individuals (September 2014) https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf

[25] The Scottish Government – Public Acceptability of Data Sharing Between the Public, Private and Third Sectors for Research Purposes (2013) http://www.gov.scot/Resource/0043/00435458.pdf

[26] Information Commissioner's Office – Annual Track organisations (June 2013) https://ico.org.uk/media/about-the-ico/documents/1042361/annual-track-2012-organisations.pdf

[27] Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Should this be for the more serious cases? Where a security breach affects the public in more than one EU country could we take more unified, cohesive action?

Rights

63. The rights of the individual are fundamental to any data protection regime and give the public the ability to control how organisations use their personal data.

64. The current draft of the new data protection Regulation provides strengthening of individuals' rights in terms of control over the processing of their personal data, as it is the organisation that will need to justify the continuance of the processing rather than the individual having to demonstrate that their objection is justified. However the research and studies indicate that the public are currently facing difficulties in exercising their current rights and there are signs that their views on rights in future are very different to the views of organisations.

Access

65. The right of access to personal data has always been the cornerstone of the data protection rights for individuals. By being able to access a copy of the information an organisation holds about them, the individual is empowered to check that the information held is accurate, relevant and not excessive.

66. In UK research[28] 62% of respondents were aware that they have the right to see the information held about them by organisations and 12% of respondents had made a request to an organisation to see what information may be held about them. That means 6 or 7 million requests within the UK – are DPAs equipped and ready to deal with the higher number of complaints that could follow if the numbers increase?

67. Research by the European academic consortium IRISS[29] into access rights found that in 20% of cases the information provided by organisations to the public about how to make a subject access request was of such poor quality that it was not possible for their researchers to identify a competent officer within the organisation in

[28] ICO - Annual Track individuals (September 2014) https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf

[29] IRISS consortium - Recommendations to the Council of the EU and the European Parliament on access rights, in the context of the European data protection reform' (31 January 2015) http://irissproject.eu/wp-content/uploads/2015/02/IRISS-POLICY-BRIEF.pdf

order to submit an access request. They found there was a vicious circle in which organisations fail to inform the public of their rights or how to access them and as a result the public do not know about a right of access meaning that few access-related queries are received from the public therefore the organisation has little motivation to train or inform their staff about data protection. The research concluded that organisations must clearly describe their subject access procedures and policies and provide explicit protocols for submitting an access request.

68. There is clearly a strong need for DPAs to ensure that both the public and organisations are educated about access rights. DPAs also need to send a strong message to organisations about the consequences of non-compliance.

69. In Eurobarometer research[30] when respondents were asked whether they thought their data would be better protected in large companies if these companies were required to have a specific person in charge of ensuring personal data is handled properly (a data protection officer) 88% agreed. As it currently stands in the new Regulation large organisations will be required to have an employee responsible for data protection.

70. However the IRISS research recommended that there was no minimum criteria for the appointment of data protection officers, as currently outlined in the draft regulation. Rather, all organisations processing personal data should have as a minimum standard a nominated officer who is trained in data protection matters and can respond to access requests, not necessarily a dedicated data protection officer only dealing with data protection matters. This could simply be a member of staff with other existing duties who has received sufficient training to deal with data protection matters such as responding to requests.

71. Research in the UK[31] found that the vast majority of companies with over 250 employees, or who keep more than 100,000 records already employee staff with a job role focused on data protection. In addition the research also found that organisations who perceive a greater risk for their business from breaches of data security or concerns about data security are more likely to have staff with a job role focused on data protection compliance.

[30] Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
[31] ICO – Implications of the European Commission's proposal for a general data protection regulation for business (May 2013) https://ico.org.uk/media/about-the-ico/documents/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf

72. Symantec research[32] recommended that organisation's front line customer services should be able to answer questions on data security and privacy and customers should be provided with an identified data privacy contact point within the organisation.

> There is an argument that more needs to be done to make the 'classical' right of subject access work better - to meet individuals' changing expectations that are being shaped by technology. People expect real-time, for free parcel-tracking and access to their bank-accounts and online order history. Perhaps DPAs should be doing more to encourage the development of much more powerful, faster and cheaper access rights for the public. Should the public have to make multiple access requests when their data is shared between a number of organisations?

Right to object - Deletion

73. It can be difficult for the public to request, and achieve, deletion of data from social media websites and other online services, and it can be difficult to regain control of personal data if for example an individual provides their data to an organisation but fails to opt-out of having their personal data passed to third parties.

74. In regard to the proposed 'right to be forgotten' the public see this as a positive. Eurobarometer research[33] found that the majority of respondents (75%) wanted to delete their personal data on a website whenever they decide to do so.

75. However it appears that organisations may not share the same positive view. Research from the UK on the views of organisations about the implications of the new Regulation on businesses[34] found that the 'right to be forgotten' was considered to be over-ambitious and impractical, and moreover, in an environment where data can be replicated and divulged in seconds it is found to be misleading and place "*unrealistic expectations*" on organisations.

76. In the ICO focus group research[35] the majority of the public believed that they should be able to remove their personal data from the public domain including social media sites if they wanted to.

---

[32] Symantec - State of Privacy Report 2015 (February 2015) http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf

[33] Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[34] ICO – Implications of the European Commission's proposal for a general data protection regulation for business (May 2013) https://ico.org.uk/media/about-the-ico/documents/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf

[35] ICO - Consumer attitudes to privacy and data protection (April 2015)

However, they did not know how they would go about it. There is therefore clearly more work for DPAs and organisations to do to educate the public on this subject.

How do we manage public expectations in this area? We know how hard – or impossible - it can be for well-resourced and determined people to have information about them deleted effectively from the internet. The recent Google Spain judgement has made us consider some difficult issues regarding the territorial reach of EU law. What can we deliver to members of the public who may well have suffered severe detriment as the result of information posted about them? How do we apply the learning from implementing the Google Spain judgment in other scenarios, beyond search engines, eg social media?

Portable personal data

77. The new Regulation proposes new rights for individuals that in effect means that their personal data will become portable between organisations should the individual require this.

78. Respondents in the Eurobarometer research were asked how important they felt it was to be able to transfer their personal data that was stored or collected through a website when they change providers or stop using a service and 71% agreed it was important to them.

79. Whilst the public appear to see portability as important, respondents to UK research on the implications of the new Regulation on businesses felt that the provision on data portability may induce customers to swamp companies with requests to have their personal data made available to them in an agreed format to reuse, putting severe strain on their resources (particularly for small to medium enterprises).

There is a balance to be struck between making it easier for the public to move their personal data around, the risks of increased data flows, particularly involving third parties, and whether it is workable for all categories of organisation and data. What more can DPAs do to educate organisations on new portability responsibilities and ensure that they are ready for the new requirements of the Regulation?

What do the public want from DPAs?

80. Data Protection Authorities (DPAs) have an important role to play, both as educator and enforcer of data protection law. In the ICO public focus group research[36], participants felt that a data protection regulator should be "*international, flexible, dynamic and independent*".

81. There are a range of examples of how DPAs are improving the way they educate and enforce however there is still room for improvement and there are a number of areas which should be developed.

82. We need to be able to understand what the public want from us in order to effectively uphold their data protection rights.

Independence

83. The role of DPAs is to ensure that private organisations and public bodies (including governments) are complying with data protection legislation. Article 28 of Directive 95/46 EC states that DPAs "*shall act with complete independence in exercising the functions entrusted to them*". The public needs to have faith in DPAs as credible regulators that are independent of outside influence and political agendas. This independence from the state is particularly important as DPAs are required to consider data protection breaches by government.

84. UK research[37] found that 79% of respondents believed it was important that the data protection enforcer is independent of government and business.

85. The independence of some DPAs has been called into question by the public and indeed by the European Commission. There have been concerns that DPAs' governing staff are appointed by political bodies, or that it is supervised by a specific government ministry, or appears to take limited action against other public institutions where there has been a data protection breach[38].

[36] ICO - Consumer attitudes to privacy and data protection (April 2015)
[37] ICO - Annual Track individuals (September 2014) https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf
[38] FRA – Access to data protection remedies in EU Member States (2013) http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en_0.pdf

86. Likewise the Court of Justice of the European Union has underlined in decisions[39] that DPAs have to remain free from any external influence, including the direct or indirect influence of the State. The mere risk of political influence through the State is sufficient to hinder the independent performance of the DPA's tasks.

87. It may be difficult for DPAs to change the way they are governed as this might be outside of their control. However DPAs should be vocal in their attempts to distance themselves and indeed resist outside influence which seeks to undermine their independence where necessary.

88. The view from FRA research[40] was that improvements need to take place in regard to the independence, effectiveness and resources and powers of DPAs. It agreed that DPAs play a crucial role as guardians of data protection in the eyes of the public and that the whole data protection system depends on public trust of DPAs. However the research concluded that it would be difficult to convince the public that their data protection concerns are being taken seriously if there are doubts about the independence of DPAs or if they do not appear to be resourced properly in order to allow them to discharge their duties efficiently and effectively.

89. As public sector budgets remain under pressure DPAs are likely to continue to face the prospect of financial restraints which means that it could be problematic in the future for DPAs to properly resource all the work they would ideally like to do.

90. FRA research into the role of national data protection authorities found that in several DPAs understaffing and a lack of adequate financial resources constitutes a major problem. It also found that control over financial resources was a relevant element in ensuring the autonomy of DPAs. This point raised again by the FRA in their subsequent remedies report.

91. The new Regulation is seeking to strengthen the independence of DPAs, for example by requiring member states to ensure that DPAs are provided with adequate resources. However, for example, in the UK the proposed abolishment in the draft Regulation of the general notification obligation whereby DPAs can charge organisations a fee poses questions about adequate future funding because currently all of the ICO's data protection work is funded by notification. This could

[39] European Commission v. Federal Republic of Germany (C-518/07 of 9 March 2010); European Commission v. Republic of Austria (C-614/10 of 16 October 2012); European Commission v. Hungary (C-288/12 of 8 April 2014).
[40] FRA 'Data Protection in the European Union: the role of National Data Protection Authorities (2010) http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

cause problems for the independence of DPAs as they are more reliant on Government for their budget and of course would have a knock on effect to the budget of the DPA more generally as there is less money to spend.

It is welcomed that the new Regulation will require member states to provide DPAs with adequate resources but how do we define adequate resources and how can we make the case for this in pressing financial times? Member states are unlikely to put the needs of DPAs over other spending such as health and welfare. Therefore what other ways could we look at to ensure the necessary funding? Is there scope for DPAs to retain the income from fines, or a proportion of them? Or recover our costs from certain investigations? Or could we start to charge for certain services which we provide, for example audits?

Consistency

92. A consistent, approach across EU DPAs is essential, whilst respecting differences in national cultures and legal systems. Currently there is a great deal of inconsistency from DPAs across Europe due to differences in the way in which Directive 2002/58/EC has been implemented into national laws. IRISS research[41] found that the spirit of the Directive has often been diminished because of the way it has been transposed into the national legal framework and sometimes further undermined by national case law.

93. Whilst the introduction of a data protection Regulation should assist with consistency of data protection rights across the EU and reduce fragmentation, implementation is not imminent and there is a good chance that a considerable degree of national variation in the way data protection law is implemented will remain.

94. Business is a global affair with large numbers of multi-national organisations operating across Europe. It can be confusing for the public – and indeed for DPAs - to understand the ownership structure of these organisations and work out which country's laws the organisation should be complying with. This confusion has been noted in the IRISS research which found that in regard to access rights there is a lack of clarity as to which national legislation, if any, international companies are subject to.

[41] IRISS consortium - Recommendations to the Council of the EU and the European Parliament on access rights, in the context of the European data protection reform' (31 January 2015) http://irissproject.eu/wp-content/uploads/2015/02/IRISS-POLICY-BRIEF.pdf

95. The inconsistency of approach to data protection across the EU can also increase bureaucracy for multi-nationals as they are likely to need to ensure compliance with a different set of data protection requirements in each country they operate in. Some multi-nationals have been able to make the current system work, through establishing contacts with a number of DPAs and pooling the understanding they gain from this. Issues about inconsistencies are then sometimes fed back to the DPAs.

96. It would be beneficial for the public to see an appropriate degree of consistency between EU DPAs. The implementation of the data protection Regulation is something which both the public and organisations are likely to welcome. When considering the public's use of the internet Eurobarometer research[42] found that even though a majority of internet users feel responsible themselves for the safe handling of their personal data, 90% of respondents would be in favour of equal protection rights across the EU.

However, the 'consistency agenda' touches on some difficult issues. For example if an aspect of an internet service is unavailable in one Member State does that necessarily mean it should be unavailable in all of them?

Visibility

97. A DPA can be incredibly well-resourced and knowledgeable however its purpose as educator is not met if it is invisible to the public. It is essential therefore that the public (and indeed organisations) are aware that there is a DPA in their country of origin. DPAs should be empowering the public so that they are aware of their rights, can exercise them, know when their rights have been breached and understand how to seek remedies. However, we also need to be able to cope with the pressures that a more prominent public profile will place on us.

98. In practice however, whilst the public tend to be are aware of data protection they are overwhelmingly unaware that DPAs exist. A Eurobarometer study[43] found that only 33% of the Europeans surveyed were aware that a national public authority responsible for protecting their rights existed.

[42] Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
[43] Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

99. Recent research in the UK[44] also confirms that DPAs could do more to engage the public as despite 97% of respondents saying when prompted that they were aware of data protection, when they were subsequently asked to choose from a list of where they would go to get advice on their rights on protecting their personal data only 1% selected the ICO (the UK DPA).

100. FRA research[45] found that most of the individuals interviewed maintained that they were not well informed about data protection breaches and the redress available and did not know where to go to find information. It also found that the main criticisms of DPAs from intermediaries (ie civil society organisations) focused on poor communication, and insufficient transparency and contribution to public awareness raising. The research concluded that DPAs should pay particular attention to cultivating their public profile and focus on raising awareness of their existence and role.

101. It is clear therefore that DPAs have a great deal of work to do to increase their visibility and to engage successfully with the public. It is open to debate as to how best to do this but clearly new and novel ways are needed to reach out to the public.

102. As a large majority of the public are accessing the internet every day it is essential that DPAs have a good digital reach, whilst not forgetting the many elderly people and others who do not have internet access. As well as having a website this should include using other forms of digital communication to promote themselves such as social media.

ICO example

The ICO operates a website[46] however it is understood that many people will not necessarily know to visit the website directly but will instead use search engines to search on a data protection or privacy issue that concerns them. The ICO therefore uses organic search engine optimisation techniques (eg optimising the website for certain key words etc) to improve its website rankings in search engines, so that more people are able to access the ICO's advice.

In addition to a website, the ICO uses a variety of other electronic means to connect with the public and organisations. These include an 'e-newsletter' which organisations/the public can subscribe to,

[44] ICO - Annual Track individuals (September 2014) https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf
[45] FRA – Access to data protection remedies in EU Member States (2013) http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en_0.pdf
[46] www.ico.org.uk

regular blog postings, and webinars.

In order to connect with more people and increase the ICO's chances of exposure to data protection issues which are already being discussed the ICO also has a presence on digital platforms;


/iconews


@iconews

103. DPAs are increasingly realising that children and young people should be specifically targeted with awareness campaigns as their use of online services can become a way of life from an early age and often have a greater online presence than many adults. The public appear to agree with this as UK research[47] found that 82% of respondents felt that it was important that schools taught children to learn how to protect their personal information and give pointers on where to go for help, information and advice.

104. Research by CNIL[48] looked at digital education across DPAs and found that a variety of different methods were being used to engage with children and young people. It recommended that all of the educational resources mentioned by the DPAs during the research be placed onto a platform which is accessible to all DPAs.

105. The ICO has conducted research[49] about embedding information rights into schools and found that whilst this would assist children in understanding their rights (which in itself is important given children are likely to be using social media) it is also likely to provide knowledge and skills for life and for their future employment.

ICO example
The ICO has developed a section of its website containing resources for schools[50] which includes lesson plans that have been developed by teachers and tailored to specific areas of the curriculum. The focus of the plans is to help children and young people better understand the value and importance of their

[47] ICO - Annual Track individuals (September 2014) https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf
[48] CNIL – International Enquiry concerning Initiatives Conducted by Data Protection Authorities with Regard to Digital Education Provisional Summary Report (4 July 2014)
[49] ICO – Embedding Information Rights into UK Education (31 March 2012) https://ico.org.uk/media/about-the-ico/documents/1042368/embedding-information-rights-phase-2-report.pdf
[50] https://ico.org.uk/for-organisations/resources-for-schools/

personal information, know how to look after it and understand the obligations that organisations have.

This content became available to schools in late 2013 and since then it has been viewed, and the resources downloaded, thousands of times and has been subject to much positive feedback from schools and teachers.

106. The visibility of DPAs to organisations also plays an important part in ensuring that the public can exercise their rights. The role of promoting and teaching organisations not only what the law requires but also good practice is essential, because organisations with low levels of awareness are more unlikely to ensure the public's data protection rights are respected. For example the IRISS research[51] found that the difficulties faced by data subjects when exercising their right of access was often compounded by an endemic lack of awareness among organisations about data protection requirements and specifically about the right of access.

ICO example
The ICO uses variety of different techniques to raise organisational awareness and help organisations improve their data protection obligations.

The ICO provides tools for organisations to use themselves to remind and train their staff on data protection issues, these include training videos, e-learning modules and promotional posters and checklists[52].

In terms of a more 'hands on' approach the ICO conducts advisory visits[53], the aim being to give small and medium sized businesses, charities and not for profit organisations practical advice on improving their data protection practice. The ICO also offers audits[54] which provide a more detailed assessment of whether an organisation is following good data protection practice and includes recommendations on how to improve. As the ICO is only able to audit a limited number of organisations each year, it publishes reports detailing some of the good practice and areas for improvement it has seen in specific sectors in order to provide

[51] IRISS consortium - European Policy Brief - Recommendations to the Council of the EU and the European Parliament on access rights, in the context of the European data protection reform (31 January 2015) http://irissproject.eu/wp-content/uploads/2015/02/IRISS-POLICY-BRIEF.pdf
[52] https://ico.org.uk/for-organisations/improve-your-practices/
[53] https://ico.org.uk/for-organisations/improve-your-practices/advisory-visits/
[54] https://ico.org.uk/for-organisations/improve-your-practices/audits/

guidance to those organisations that have not undergone an audit.

The ICO has targeted specific sectors and worked with industry bodies to promote good data protection practice by their members. For example the ICO worked with the Local Government Association (a membership organisation that works on behalf of local councils) to issue a joint letter[55] to its members to urge them to take stock of how they meet their data protection obligations and exercise their governance obligations in this area.

107. The participants in FRA research[56] considered it was important that DPAs raise organisational awareness about the legislation and its application.

ICO example

The ability of the ICO to undertake data protection audits and advisory visits for all the organisations it regulates is limited by its resources. Therefore over the last 18 months, the ICO has been developing an online data protection Self-Assessment Toolkit aimed at small and medium sized organisations. The objective is to give more organisations the opportunity to evaluate and benchmark their own data protection compliance without the direct involvement of the ICO – to self-assess their compliance with data protection.

The Toolkit has 5 main checklists that organisations can complete;

- Data protection assurance;
- Information security;
- Records management;
- Data sharing and subject access; and
- Direct marketing.

Each of the five main checklists contains subsets of controls. The subsets consist of individual measures against which an organisation should assess themselves using the options provided. Each measure also contains some 'more information' which includes further explanation and suggestions that should be considered when making the assessment, as well as some 'guidance' links which provide additional relevant references.

[55] https://ico.org.uk/media/about-the-ico/documents/1042567/lga-and-ico-letter-to-council-leaders.pdf

[56] FRA – Access to data protection remedies in EU Member States (2013) http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en_0.pdf

For each completed checklist the Toolkit will generate an assessment rating based on the organisation's responses as well as an overall rating using a simple 'traffic light' (red/amber/green) system.

The ICO will shortly launch a pilot programme to test the toolkit with a small number of volunteer organisations prior to a general release on the ICO website later this year.

108. For those organisations that deliberately ignore the public's rights a visible DPA demonstrating firm enforcement messages is very important. We will consider enforcement later in this paper.

109. The new Regulation makes it even more imperative for DPAs to engage with organisations about their responsibilities – explaining how their compliance obligations will remain the same or where they may change.

110. Research in the UK commissioned by the ICO[57] about the implications of the proposal for a general data protection regulation on businesses cast light on the level of uncertainty that exists within the UK business population regarding the scope of the Regulation and its cost impact. It found that the lack of understanding about the provisions in the draft Regulation persists across business indicated that there is a key role for the ICO to play in educating and supporting businesses to increase their awareness and understanding of their obligations as a result of the forthcoming changes. Of course, though, businesses cannot be expected to put resource into detailed future compliance programmes until they know exactly what will be expected of them. At this stage organisations should have a reasonable understanding of the general direction and where continuity is likely or possible new areas. There is a case to be made about how positive compliance with current data protection legislation now will aid compliance with the new Regulation.

111. There are of course likely to be resource implications on DPAs if they try to make themselves and data protection rights more visible in terms of costs and staff time, and ultimately where budgets are scarce DPAs may simply be unable to devote the time and money necessary to promote their visibility.

[57] ICO – Implications of the European Commission's proposal for a general data protection regulation for business (May 2013) https://ico.org.uk/media/about-the-ico/documents/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf

112. It is essential therefore that DPAs look for opportunities to increase their visibility in a way which is sustainable within financial restraints.

113. This could be by closer co-operation between DPAs. DPAs all have the same common goal so it is only right and sensible that we learn from each other and are able to pool publications, initiatives etc where these have been proved to be successful in engaging the public and organisations. There have already been examples of this; research by CNIL[58] found that a publication by the Irish DPA ('*Sign up, Log In, Opt out – Protecting your Privacy and controlling your data*') aimed raising young people's awareness of their right to privacy had been reproduced and translated by several other DPAs. There were also other indications in the CNIL research that some DPAs had pooled resources to organise study days, conferences or joint work.

114. Other examples include co-operation on the Google Privacy Policy Taskforce and case handling workshops where case handling expertise is shared between DPAs – as seen at the Spring Conference. There is also the new Article 29 Working Party sub group on co-operation for items such as a common typology of DPA activities.

115. It is not just closer co-operation between EU DPAs as organisations operate globally, DPAs should therefore look for opportunities to work with authorities outside of the EU. There are already examples of closer international co-operation for example the annual Global Privacy Enforcement Network[59] sweep in which privacy enforcement agencies in numerous countries search websites and apps in a co-ordinated way during a week of May, to assess privacy practices.

116. Another alternative could be working with partner agencies to target specific sectors and cover specific issues which involve data protection and privacy. So for example issuing joint guidance with specific sector's regulator or providing input to guidance and publications created by a charity in relation to specific scenarios involving data protection.

> **ICO example**
> The ICO worked with the Alzheimer's Society (a UK dementia charity) on a publication called '*Accessing and sharing information: acting on behalf of a person with dementia*'[60]. The

[58] CNIL – International Enquiry concerning Initiatives Conducted by Data Protection Authorities with Regard to Digital Education – Provisional summary report (4 July 2014)
[59] https://www.privacyenforcement.net/
[60] https://iconewsblog.wordpress.com/2015/02/11/how-data-protection-helps-supporting-someone-with-dementia/

ICO's role was to advise on how data protection works in the scenarios presented by the publication.

The ICO had become increasingly aware of data protection concerns being reported by the public in relation to problems they were encountering when trying to engage with organisations on behalf of family and friends with dementia. Complaints and enquiries received by the ICO showed there was a good deal of uncertainty in this area, as well as highlighting instances where people with a power of attorney have been denied access to information about the people they represent. The charity's leaflet was a good opportunity for the ICO to get involved and help set out clear guidelines in relation to data protection.

117. DPAs may consider taking a strategic approach when deciding where to aim their resources, therefore being 'selective to be effective'. Taking a risk based approach and for example targeting the particular organisational sectors which cause the most complaints or which have the greatest potential security risks etc.

ICO example
The ICO faces rising demand for everything it does and uncertainties over funding. The ICO set itself a strategic objective of having "*an operations directorate that is focused on improving information rights practices amongst organisations*".

To meet this strategic objective the ICO initiated a review of the way it works to ensure it was delivering value for money and fulfilling its corporate obligation to be a modern and effective regulator. This was referred to as 'Project Eagle' and the objectives of the project were to;

- Have a practical method of deciding which issues raised by the public are taken forward;
- Have a defined approach for gathering and analysing information to help co-ordinate its efforts to improve Information Rights practice;
- Have an efficient process in place to manage workflow so it can cope with volume throughout the year; and
- Manage expectations and ensure it provides a high standard of service whilst delivering its new strategic objective.

The new way of working was implemented on April 2014 and six months later there was a reduction of ineligible complaints made

to ICO. This appears to be due to changes made to the ICO's website, including a guided user journey that assists people in reporting concerns[61], and the advice provided on the ICO's helpline which is better at encouraging the public to raise their concerns with the organisation before contacting the ICO. Alongside this, the changes to the way of working were promoted externally to organisations which hopefully encouraged them to better deal with public concerns.

For example, the ICO analysed the concerns it received about lenders in the banking and finance sector, and challenged the sector to better explain their information rights practices to customers. As a result this year the ICO has dealt with over 700 fewer concerns about lenders; a significant reversal of recent trends.

118. Even where DPAs do have the means by which to increase their visibility there is still a risk to their resources if they become highly prominent to both the public and organisations. The risk to DPAs is that they become a victim of their own success and are overwhelmed by enquiries and complaints which they cannot cope with. Greater visibility must therefore go hand in hand with adequate resources and DPAs need to ensure that consideration has been given as to how they would cope in the event that their visibility campaign is a success.

What techniques work best to improve the visibility of DPAs, what are the most cost effective? How can DPAs best share knowledge and experience of these techniques?

Privacy certification, seals and trust marks

119. As discussed earlier in this paper, the public have a general lack of trust that organisations will use their personal data only for the purposes for which it was collected. We have also seen that the public, if they do read privacy notices, often do not understand what they are reading.

120. The public are used to seeing certification and trust marks in their daily lives on both a national level (eg in the UK there is a Kitemark symbol used by the British Standard Institute[62] on products and services to demonstrate quality and assurances of high standards)

[61] https://ico.org.uk/concerns/
[62] http://www.bsigroup.com/en-GB/

and on a European level (eg the 'CE marking' which signifies that products sold in the European Economic Area have been assessed to meet high safety, health, and environmental protection requirements[63]). Having certification marks provides an easy point of reference for the public and can give them confidence that an appropriate body has checked that the correct standards have by reached by the organisation.

121. In Article 39 of the new Regulation the possibility to establish certification mechanisms and data protection seals and marks is introduced. This provision gives an opportunity for DPAs to extend their reach in promoting compliance and assist in increasing public trust in organisations' handling of personal data.

122. There is support from the public for a data protection certification mark in the UK. Research respondents were shown examples of certification marks and were asked to what extent they would approve or disapprove of a similar certification mark being introduced to show that an online service provider has been certified in protecting information rights - 81% of respondents approved of such a system[64].

ICO example – UK privacy seal scheme

What is the ICO doing?
The ICO is currently developing plans to introduce a consumer-facing privacy seal in the UK. A privacy seal is a 'stamp of approval' which demonstrates good privacy practice and high data protection compliance standards, going beyond the letter of the law where possible.

What are the benefits for consumers and organisations?
The aim of the initiative is to raise awareness of privacy concerns, encourage transparency by organisations and build consumer trust and choice. The presence of a seal will highlight those organisations that go the extra mile to look after people's information and potentially provide them with a competitive advantage. A privacy seal will raise the bar for privacy standards across the UK and will help protect personal information.

How will it work?
The ICO will endorse third party operators to deliver privacy seal schemes. It is anticipated that there will be a number of scheme

[63] http://ec.europa.eu/growth/single-market/ce-marking/index_en.htm
[64] ICO - Annual Track individuals (September 2014) https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf

operators running schemes focused on different sectors, processes, products or areas of compliance.

Scheme operators must be accredited by the national accreditation body[65] to the relevant ISO standard (ISO 17065 – Conformity assessment – requirements for bodies certifying products, processes and services).

Once approved, the scheme operator will have responsibility for the day to day running of the scheme. The ICO will not be involved in the operation of schemes but will maintain regulatory oversight through its complaints and enforcement remit, in line with the requirements of DPA.

Once an organisation has been assessed and certified, it will be able to use the seal externally to show it is adopting best practice when processing people's information. It is intended that an organisation would only certified for a certain period of time (likely to be four years) before revalidation would be required. The seal could also be removed from an organisation if they subsequently fail to maintain the required standards (eg if they suffer a serious personal data breach).

123. As we have already discussed resources place a major obstacle to DPAs, limiting the work which we are able to do. Therefore given the lack of resources it is likely to be impractical for DPAs to take on the assessment of every organisation who seeks privacy certification. Partnering with a third party or parties that have been delegated responsibility for the running of the privacy seal scheme – ie a co-regulatory approach - is one way forward (as in the above example).

However should we being looking for greater co-operation between ourselves with such schemes? As the new Regulation will bring greater harmony between Member States should we be considering a single European privacy seal recognised by every DPA? Would this be of benefit to the public and to business? Or is there a danger that such a scheme becomes unnecessarily bureaucratic?

[65] United Kingdom Accreditation Service (UKAS) formally appointed as the National Accreditation Body for the United Kingdom, under EU Regulation 765/2008 (www.ukas.com)

Responsive to new technologies

124. Increasingly the world is becoming a much more technologically advanced place, with a seemingly endless stream of new technology (eg the 'internet of things'). The public's daily lives increasingly take place online (eg internet shopping, banking, e-learning and social media), all contributing to new privacy challenges.

125. According to the recent Eurobarometer 'Cyber security' report[66] 63% of the respondents use the internet every day which is an increase of 9% on their previous report in 2013. This Eurobarometer study also reported that as well as 92% of respondents accessing the internet from a computer, 61% use a smartphone and 30% use a touchscreen tablet. The use of smartphones and tablets has increased dramatically since the 2013 study (up from 35% and 14% respectively in their previous report). This has implication for transparency and how privacy notices are delivered on small-screen devices.

126. Whilst the use of the internet and new technologies continues to increase it is interesting to note that type of organisations least trusted by the public according to Eurobarometer research[67] are those involved in the online and technical sector; 22% of respondents trust internet companies eg search engines, social networking sites and email services, and 32% trust telephone/mobile companies and internet service providers.

127. This is similar to the views of respondents from the Symantec research[68] which found that only 22% trusted 'tech companies' to keep data completely secure and only 10% trusted social media organisations. Likewise in UK research[69] when respondents were asked to pick from a list of types of organisations which they would be most concerned about holding their personal information 64% picked search engines and social media networks.

128. It appears that the public's distrust of internet/technology companies may be based from experience. In FRA research[70] internet based activities emerged as a high risk area for data protection breaches as

[66] Special Eurobarometer 423 – Cyber security (February 2015) http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf
[67] Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
[68] Symantec - State of Privacy Report 2015 (February 2015) http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf
[69] ICO - Annual Track individuals (September 2014) https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf
[70] FRA – Access to data protection remedies in EU Member States (2013) http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en_0.pdf

the most frequent data protection breaches mentioned by respondents were those related to internet based activities including for example social media, internet shopping and email accounts. As a result of their experiences these respondents were of the opinion it was essential that the resources of DPAs should include strong technical departments with access to the latest technology.

129. It is important that DPAs ensure that they are responsive to new technologies and the implications which these may have on the public's data protection rights. Having staff with the necessary technical expertise to deal with data protection matters which involve detailed technical issues is vital to ensure that the DPA can reach fully informed conclusions.

ICO example
As is the case in a number of European and international data protection and privacy enforcement agencies having 'in-house' technology experts is of critical importance to provide technical and information security expertise.

The ICO has a small team of specialist staff who not only advise on the technical aspects of complaints received and data breach investigations but they also input into the technical advice and guidance delivered to organisations and members of the public. They also monitor the technology environment to identify the developments which may impact on information rights. In order to assist the work of the technology team the ICO also has a dedicated computer lab which allows the technology team to perform a closer inspection of the technology they are reviewing.

130. Resources again may present a barrier to how effectively DPAs can respond to the data protection challenges which new technologies bring.

So what can we do so as not to be left behind by technical advancement? Is there a further opportunity for greater co-operation and knowledge sharing between DPAs?

Enforcement

131. Promoting good data protection practice by providing the appropriate tools and guidance to organisations is only part of what is required to ensure the public's personal data is protected. There also needs to be the right tools and sanctions available to deter organisations from

wilfully ignoring data protection responsibilities and to ensure that data protection is taken seriously by organisations.

132. Who does the public think should enforce data protection breaches? There is no clear consensus of opinion from the public as Eurobarometer research[71] found that 44% of respondents would prefer the European level of administration for enforcing regulation whilst 40% would prefer the national level.

133. In FRA research on 'Access to data protection remedies in EU Member States remedies'[72] many respondents from different countries said they lacked trust in the effectiveness of the remedies in the area of data protection or in public institutions in general and for some those doubts stopped them from initiating the redress procedure.

134. On occasion the public have taken matters of data protection and privacy into their own hands through the courts. A high profile example in the UK is Vidal-Hall vs. Google Inc[73] which looked at Google collecting private information about the claimants' internet usage via their Apple Safari browser without the claimants' knowledge and consent, by using a small string of text saved on the user's device ('cookies'). The ICO successfully intervened in this case in the Court appeal – the Court agreed with our arguments that unique browser generated information was personal data and compensation could be awarded for distress alone, rather than for financial damage.

135. In another case (Schrems vs. Facebook) the claimant is seeking a declaration that the safe harbour designation under EU law should be cancelled. This case has recently been heard by the Court of Justice of the European Union and a ruling is awaited.

136. In the Eurobarometer research when respondents were asked about what type of regulation should be introduced to prevent organisations from using personal data without the person's knowledge 51% thought that these companies should be fined, 40% thought they should be banned from using such data in the future and 39% thought they should be compelled to compensate the victims.

---

[71] Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[72] FRA – Access to data protection remedies in EU Member States (2013) http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en_0.pdf

[73] UK Court of Appeal - A2/2014/0403 [2015] EWCA Civ 311 (27 March 2015) https://www.judiciary.gov.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf

137. The FRA research found that in the opinion of their respondents financial compensation was not a motivating factor to seek redress, instead most cited a desire to ensure that similar breaches do not recur.

138. In separate FRA research on 'Data Protection in the European Union: the role of National Data Protection Authorities'[74] it was found that there was a general tendency in the Member States to focus on 'soft' methods of securing compliance with data protection legislation, instead of applying and enforcing 'hard' instruments by which violators of data protection rights may be detected, punished and asked to compensate victims.

ICO example
Since April 2010 the ICO has been able to issue fines (Civil Monetary Penalties - CMPs) of up to £500,000 for serious breaches of the UK Data Protection Act 1998. In February 2014 the ICO commissioned research[75] on the impact of CMPs the purpose being to review the extent to which CMPs influence or improve data protection compliance and practice by organisations.

The research indicated that CMPs are effective at improving data protection compliance and this was particularly clear for those organisations that had been issued with one. The impact was that these organisations took their data protection obligations more seriously with data protection being given a higher profile with greater senior staff buy-in. It also led to revised practices and policies, increased staff training and awareness campaigns within the organisations.

The research also confirmed that the positive impact extended to 'peer' organisations as CMPs had a wider impact as a useful deterrent and incentive to get data protection right. A substantial proportion of respondents said they had reviewed or changed their data protection practices and policies as a result of hearing about CMPs being issued to other organisations.

139. DPAs need to target their enforcement resources effectively. As has already been discussed DPAs only have a finite amount of resources to perform their functions therefore it is important that enforcement

[74] FRA - Data protection in the European Union: the role of National Data Protection Authorities (2010) http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf
[75] ICO – Review of the impact of ICO Civil monetary Penalties (23 July 2014) https://ico.org.uk/media/about-the-ico/documents/1042346/review-of-the-impact-of-ico-civil-monetary-penalties.pdf

action is used in such a way so as to provide the best value outcomes.

ICO example
The ICO's information rights strategy commits it to adopting a positive and proactive approach to ensuring compliance of organisations by:

- helping and encouraging organisations to understand and meet their information rights obligations more easily; and
- responding proportionately to breaches of information rights law.

This 'carrot and stick' approach means that the ICO will adopt a targeted, risk-driven approach to regulatory action - not using its legal powers lightly or routinely, but taking a tough and purposeful approach on those occasions where that is necessary.

The ICO has a Regulatory Action Policy[76] which sits under the umbrella of its information rights strategy. It elaborates the above approach, setting out the nature of our various powers and when and how the ICO plans to use them. It is intended that the policy sends clear and consistent signals to those who fall within the scope of the UK Data Protection Act 1998, to the public whom the law protects and empowers, and to the staff who act on the ICO's behalf. The ICO's view is that targeted, proportionate and effective regulatory action will also contribute to the promotion of good practice and ensuring it remains an influential office.

140. It would be beneficial to the public for DPAs to do more research on how their enforcement action is actually working in practice and there is opportunity for DPAs to share evidence as to what does and does not work in relation to the various types of enforcement action used.

141. The European Data Protection Supervisor's recent preliminary report on 'Privacy and competitiveness in the age of big data'[77] suggested an international approach to closer dialogue with other sectoral

[76] ICO – Data Protection Regulatory Action Policy (August 2013) https://ico.org.uk/media/about-the-ico/policies-and-procedures/1853/data-protection-regulatory-action-policy.pdf

[77] European Data Protection Supervisor – Preliminary Opinion – Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy (March 2014) https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

regulators, for example in the competition and consumer protection sectors, to agree a more holistic approach to enforcement.

It may be in the future that greater emphasis is put onto cross-border investigations which cumulate in joint enforcement action between DPAs, especially since compliance issues can cover many jurisdictions. But what are the practicalities of such a process and how do we ensure that it is of value to the public? Are we more likely to see class actions from members of the public who by-pass DPAs altogether and if so what role, if any, do we have to play in this?

The way forward

142. During this paper we have discussed the views of the public on data protection and how DPAs could endeavour to meet the expectations which are placed on them to promote and uphold data protection rights, against the backdrop of limited resources.

143. The ICO has proposed a Resolution to the EU DPAs Spring Conference about 'Meeting data protection expectations in the digital future'. This Resolution makes a call for the funding of EU DPAs to be sufficient to meet the increasing demands on them, and calls upon law makers in Europe to ensure that the next generation of data protection laws are drafted in a clear and easily understood way.

144. The Resolution reminds EU DPAs of the need to raise public awareness, target their finite resources appropriately to achieve genuinely protective outcomes for individuals, to work with third parties (including other DPAs) to amplify data protection messages, and encourage the development of data protection and privacy enhancing mechanisms. It also reminds DPAs of the need to develop systematic and proactive approaches to tackling non-compliant behaviour, be more responsive to new technologies, be assertive in making the case for resources, and to continue to develop Europe-wide co-operation initiatives to share information and knowledge about practical approaches to data protection.