

Regulator Assessment: Qualifying Regulatory Provisions

Title of proposal	A practical guide to IT security
Lead Regulator	Information Commissioner's Office (ICO)
Contact for enquiries	Carl Wiper, Group Manager, Policy Delivery carl.wiper@ico.org.uk tel 01625 545503

Date of assessment	21 March 2017
Commencement date	6 January 2016
Origin	Domestic
Does this include implementation of a Cutting Red Tape review?	No
Which areas of the UK will be affected?	All

Brief outline of proposed new or amended regulatory activity

This is a guidance document, aimed principally at SMEs. It provides practical advice on IT security measures which they can take in order to safeguard personal data. The Data Protection Act 1998 (DPA) requires those processing personal data to take appropriate technical and organisational security measures against unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to personal data. This document provides good practice advice on how to meet this requirement. It does not impose any obligations beyond those in the DPA.

Which type of business will be affected? How many are estimated to be affected?

This guidance is potentially relevant to all businesses that process personal data, ie most if not all businesses in the country. However, businesses are not *required* to read this guidance or to implement its recommendations in order to meet their obligations under the DPA. We have therefore based our estimate of the number of businesses affected on an estimate of the number who have accessed the guidance via our website. This produces an estimate of 842 businesses.

Summary of costs and benefits

Price base year	Implementation date	Duration of policy (years)	Net Present Value	Business Net Present Value	Net cost to business (EANDCB)	BIT score
2014	2016	5	0	0	0	0

Please set out the impact to business clearly with a breakdown of costs and benefits

This document makes recommendations but it does not require business to do anything, beyond the requirements in legislation. We determine therefore that as the guidance allows businesses to act, that it is permissive in nature. It is therefore not possible to estimate in any meaningful way the cost/ benefit to business of taking any action as a result of reading our guidance. There is currently no further evidence available of the cost to business and we believe that it would be disproportionate to attempt to collect further evidence.

It is only possible to estimate the cost of reading the document itself. We therefore consider the impact to business to be the cost of reading the guidance. We believe this approach to be consistent with the document *Draft appraisal of guidance* published by BEIS on the Alfresco collaboration site.

Using the Standard Cost Model, we have calculated the cost of reading the guidance as follows:

We calculated the Estimated Time to Read (ETTR) the document, by obtaining the Fleisch Reading Ease (FRE) score (using the spelling/ grammar checker in MS Word) and using this to obtain the number of words per minute (using the table in *Draft appraisal of guidance*). Our guidance documents typically fall within the FRE range 30-70; we have taken FRE 30-50 as equivalent to 75 wpm, FRE 50-60 as equivalent to 100 wpm and 60-70 as equivalent to 200 wpm. We then multiplied the wpm by the word count to obtain the ETTR in minutes.

In order to estimate the number of businesses reading the guidance, we took the number of unique page views on our website in 2016 from our own web analytics. To estimate what proportion of website views came from users within businesses, we used the results of a recent ICO website survey. Between 26 May and 9 June 2016, the ICO ran a website user survey, published on the ICO website and publicised through social media channels. During this period, the ICO received 1,741 survey responses, identifying that 48% of users were from organisations and 23.7% of users were from private sector organisations. We therefore multiplied the number of unique page views by 23.7% to determine the number of views from businesses.

We have no way of knowing who within a business is reading our documents and so we have assumed that the typical reader is a manager. We have used the mean hourly wage cost for a manager from the Annual Survey of Hours and Earnings (ASHE) of £24.81 and added 20.2% of the wage cost for on-costs. This 20.2% figure is based upon the latest Eurostat figures, which outlines that non-wage cost, as a proportion of total wage cost is 16.8%. This implies that wage costs are 83.2% of total labour cost. As outlined in the BIT assessments: models and data sources document, to calculate the wage + non-wage costs, we multiply the wage cost by $(1 + \text{non-wage cost} / \text{wage cost})$. Based on the figure of 16.8%, this works out as $\text{Wage cost} * (1 + (0.168 / 0.832))$ or $\text{Wage cost} * (1 + 0.202)$.

This gives us the hourly employment cost of a typical reader of our guidance. We have further assumed that this person reads the document once each year, for familiarisation.

In summary, the cost to business of reading the guidance in any one year is therefore:

$$\text{ETTR} \times \text{no. of businesses reading it} \times (\text{wage cost} + \text{on-cost})$$

This gives a figure of £12,146 per annum as the cost to business. The attached spreadsheet sets out the calculation in detail.

We do not believe there is a reliable way to monetise the direct benefit to business of reading our guidance. This is because it is not possible to estimate the counterfactual ie the cost to business of *not* reading our guidance. It may be assumed that, without the guidance, some businesses would pay for legal advice on the points it covers, while others may obtain advice informally from their peers, or internally eg from their data protection officer (if they have one), or simply work out for themselves what to do. The *Draft appraisal of guidance* document contains some estimates of the cost of external advice, but there is no robust way to relate this to advice on the specific points covered by the guidance. As reading the guidance is voluntary, we consider that it is reasonable to expect that business will therefore read it only where it leads to net benefits; the analysis therefore assumes that the benefits are at least equal to the costs.

For the purposes of calculating the EANDCB we have assumed policy duration of five years. This is because the guidance reflects the requirements in the period of transition from DPA to GDPR, and there is also some uncertainty as regards the long term position post- Brexit. It is reasonable to assume that we may revise the guidance after five years, if not before.

Please provide any additional information (if required) that may assist the RPC to validate the BIT Score

Regulator Assessment: Qualifying Regulatory Provisions

Title of proposal	Wi-Fi Location Analytics guidance
Lead Regulator	Information Commissioner's Office (ICO)
Contact for enquiries	Carl Wiper, Group Manager, Policy Delivery carl.wiper@ico.org.uk tel 01625 545503

Date of assessment	21 March 2017
Commencement date	16 February 2016
Origin	Domestic
Does this include implementation of a Cutting Red Tape review?	No
Which areas of the UK will be affected?	All

Brief outline of proposed new or amended regulatory activity

This is a guidance document that explains how operators of Wi-Fi and other communication networks may use location and other analytics information in a manner compliant with the Data Protection Act 1998 (the DPA). The DPA requires those who process personal data to do so in a manner that is fair and lawful and to retain personal data for only as long as necessary. This document provides good practice advice on how to meet this requirement. It does not impose any obligations beyond those in the DPA.

Which type of business will be affected? How many are estimated to be affected?

This guidance is potentially relevant to all businesses that operate a Wi-Fi network, for example, many businesses in the service industry which provide Wi-Fi for customer use. However, businesses are not *required* to read this guidance or to implement its recommendations in order to meet their obligations under the DPA, because it does not impose obligations on businesses, beyond what is in legislation. We have therefore based our estimate of the number of businesses affected on an estimate of the number who have accessed the guidance via our website. This produces an estimate of 132 businesses.

Summary of costs and benefits						
Price base year	Implementation date	Duration of policy (years)	Net Present Value	Business Net Present Value	Net cost to business (EANDCB)	BIT score
2014	2016	5	0	0	0	0

Please set out the impact to business clearly with a breakdown of costs and benefits

This document makes recommendations but it does not require business to do anything, beyond the requirements in legislation. We determine therefore that as the guidance allows businesses to act, that it is permissive in nature. It is therefore not possible to estimate in any meaningful way the cost/ benefit to business of taking any action as a result of reading our guidance. There is currently no further evidence available of the cost to business and we believe that it would be disproportionate to attempt to collect further evidence.

It is only possible to estimate the cost of reading the document itself. We therefore consider the impact to business to be the cost of reading the guidance. We believe this approach to be consistent with the document *Draft appraisal of guidance* published by BEIS on the Alfresco collaboration site.

Using the Standard Cost Model, we have calculated the cost of reading the document as follows:

We calculated the Estimated Time to Read (ETTR) the document, by obtaining the Fleisch Reading Ease (FRE) score (using the spelling/ grammar checker in MS Word) and using this to obtain the number of words per minute (using the table in *Draft appraisal of guidance*). Our guidance documents typically fall within the FRE range 30-70; we have taken FRE 30-50 as equivalent to 75 wpm, FRE 50-60 as equivalent to 100 wpm and 60-70 as equivalent to 200 wpm. We then multiplied the wpm by the word count to obtain the ETTR in minutes.

In order to estimate the number of businesses reading the guidance, we took the number of unique page views on our website in 2016 from our own web analytics. To estimate what proportion of website views came from users within businesses, we used the results of a recent ICO website survey. Between 26 May and 9 June 2016, the ICO ran a website user survey, published on the ICO website and publicised through social media channels. During this period, the ICO received 1,741 survey responses, identifying that 48% of users were from organisations and 23.7% of users were from private sector organisations. We therefore multiplied the number of unique page views by 23.7% to determine the number of views from businesses.

We have no way of knowing who within a business is reading our documents and so we have assumed that the typical reader is a manager. We have used the mean hourly wage cost for a manager from the Annual Survey of Hours and Earnings (ASHE) of £24.81 and added 20.2% of the wage cost for on-costs. This 20.2% figure is based upon the latest Eurostat figures, which outlines that non-wage cost, as a proportion of total wage cost is 16.8%. This implies that wage costs are 83.2% of total labour cost. As outlined in the BIT assessments: models and data sources document, to calculate the wage + non-wage

costs, we multiply the wage cost by $(1 + \text{non-wage cost/wage cost})$. Based on the figure of 16.8%, this works out as $\text{Wage cost} * (1 + (0.168/0.832))$ or $\text{Wage cost} * (1 + 0.202)$.

This gives us the hourly employment cost of a typical reader of our guidance. We have further assumed that this person reads the document once each year, for familiarisation.

In summary, the cost to business of reading the guidance in any one year is therefore:

$$\text{ETTR} \times \text{no. of businesses reading it} \times (\text{wage cost} + \text{on-cost})$$

This gives a figure of £1,903 per annum as the cost to business. The attached spreadsheet sets out the calculation in detail.

We do not believe there is a reliable way to monetise the direct benefit to business of reading our guidance. This is because it is not possible to estimate the counterfactual ie the cost to business of *not* reading our guidance. It may be assumed that, without the guidance, some businesses would pay for legal advice on the points it covers, while others may obtain advice informally from their peers, or internally eg from their data protection officer (if they have one), or simply work out for themselves what to do. The *Draft appraisal of guidance* document contains some estimates of the cost of external advice, but there is no robust way to relate this to advice on the specific points covered by the guidance. As reading the guidance is voluntary, based on the reasonable expectation that business will read the guidance only where it leads to net benefits, the analysis assumes that the benefits are at least equal to the costs.

For the purposes of calculating the EANDCB we have assumed policy duration of five years. This is because the guidance reflects the requirements in the period of transition from DPA to GDPR, and there is also some uncertainty as regards the long term position post- Brexit. It is reasonable to assume that we may revise the guidance after five years, if not before.

Please provide any additional information (if required) that may assist the RPC to validate the BIT Score

Regulator Assessment: Qualifying Regulatory Provisions

Title of proposal	Using the crime and taxation exemptions (Section 29)
Lead Regulator	Information Commissioner's Office (ICO)
Contact for enquiries	Carl Wiper, Group Manager, Policy Delivery carl.wiper@ico.org.uk tel 01625 545503

Date of assessment	21 March 2017
Commencement date	26 May 2015
Origin	Domestic
Does this include implementation of a Cutting Red Tape review?	No
Which areas of the UK will be affected?	All

Brief outline of proposed new or amended regulatory activity

This document is aimed at all organisations and businesses that process personal data. The Data Protection Act 1998 (DPA) outlines exemptions to its provisions, in this instance, under section 29, where data is processed for purposes connected to crime and taxation. This document provides good practice advice on how to apply this exemption to personal data that an organisation processes. It does not impose any obligations beyond those in the DPA.

Which type of business will be affected? How many are estimated to be affected?

This guidance is potentially relevant to all businesses that process personal data, ie most, if not all, business in the country. However, businesses are not *required* to read this guidance or to implement its recommendations in order to meet their obligations under the DPA, because it does not impose obligations on businesses, beyond what is in legislation. We have therefore based our estimate of the number of businesses affected on an estimate of the number who have accessed the guidance via our website. This produces an estimate of 644 businesses.

Summary of costs and benefits						
Price base year	Implementation date	Duration of policy (years)	Net Present Value	Business Net Present Value	Net cost to business (EANDCB)	BIT score
2014	2016	5	0	0	0	0

Please set out the impact to business clearly with a breakdown of costs and benefits

This document makes recommendations but it does not require business to do anything, beyond the requirements in legislation. We determine therefore that as the guidance allows businesses to act, that it is permissive in nature. It is therefore not possible to estimate in any meaningful way the cost/ benefit to business of taking any action as a result of reading our guidance. There is currently no further evidence available of the cost to business and we believe that it would be disproportionate to attempt to collect further evidence.

It is only possible to estimate the cost of reading the document itself. We therefore consider the impact to business to be the cost of reading the guidance. We believe this approach to be consistent with the document *Draft appraisal of guidance* published by BEIS on the Alfresco collaboration site.

Using the Standard Cost Model, we have calculated the cost of reading the document as follows:

We calculated the Estimated Time to Read (ETTR) the document, by obtaining the Fleisch Reading Ease (FRE) score (using the spelling/ grammar checker in MS Word) and using this to obtain the number of words per minute (using the table in *Draft appraisal of guidance*). Our guidance documents typically fall within the FRE range 30-70; we have taken FRE 30-50 as equivalent to 75 wpm, FRE 50-60 as equivalent to 100 wpm and 60-70 as equivalent to 200 wpm. We then multiplied the wpm by the word count to obtain the ETTR in minutes.

In order to estimate the number of businesses reading the guidance, we took the number of unique page views on our website in 2016 from our own web analytics. To estimate what proportion of website views came from users within businesses, we used the results of a recent ICO website survey. Between 26 May and 9 June 2016, the ICO ran a website user survey, published on the ICO website and publicised through social media channels. During this period, the ICO received 1,741 survey responses, identifying that 48% of users were from organisations and 23.7% of users were from private sector organisations. We therefore multiplied the number of unique page views by 23.7% to determine the number of views from businesses.

We have no way of knowing who within a business is reading our documents and so we have assumed that the typical reader is a manager. We have used the mean hourly wage cost for a manager from the Annual Survey of Hours and Earnings (ASHE) of £24.81 and added 20.2% of the wage cost for on-costs. This 20.2% figure is based upon the latest Eurostat figures, which outlines that non-wage cost, as a proportion of total wage cost is 16.8%. This implies that wage costs are 83.2% of total labour cost. As outlined in the BIT assessments: models and data sources document, to calculate the wage + non-wage costs, we multiply the wage cost by $(1 + \text{non-wage cost} / \text{wage cost})$. Based on the figure of

16.8%, this works out as Wage cost * (1+(0.168/0.832)) or Wage cost * (1+0.202).

This gives us the hourly employment cost of a typical reader of our guidance. We have further assumed that this person reads the document once each year, for familiarisation.

In summary, the cost to business of reading the guidance in any one year is therefore:

$$\text{ETTR} \times \text{no. of businesses reading it} \times (\text{wage cost} + \text{on-cost})$$

This gives a figure of £20,476 per annum as the cost to business. The attached spreadsheet sets out the calculation in detail.

We do not believe there is a reliable way to monetise the direct benefit to business of reading our guidance. This is because it is not possible to estimate the counterfactual ie the cost to business of *not* reading our guidance. It may be assumed that, without the guidance, some businesses would pay for legal advice on the points it covers, while others may obtain advice informally from their peers, or internally eg from their data protection officer (if they have one), or simply work out for themselves what to do. The *Draft appraisal of guidance* document contains some estimates of the cost of external advice, but there is no robust way to relate this to advice on the specific points covered by the guidance. As reading the guidance is voluntary, based on the reasonable expectation that business will read the guidance only where it leads to net benefits, the analysis assumes that the benefits are at least equal to the costs.

For the purposes of calculating the EANDCB we have assumed policy duration of five years. This is because the guidance reflects the requirements in the period of transition from DPA to GDPR, and there is also some uncertainty as regards the long term position post- Brexit. It is reasonable to assume that we may revise the guidance after five years, if not before.

Please provide any additional information (if required) that may assist the RPC to validate the BIT Score

Regulator Assessment: Qualifying Regulatory Provisions

Title of proposal	Preparing for the General Data Protection Regulations (GDPR) – 12 Steps to take now
Lead Regulator	Information Commissioner's Office (ICO)
Contact for enquiries	Carl Wiper, Group Manager, Policy Delivery carl.wiper@ico.org.uk tel 01625 545503

Date of assessment	21 March 2017
Commencement date	14 March 2016
Origin	Domestic and European Union (EU)
Does this include implementation of a Cutting Red Tape review?	No
Which areas of the UK will be affected?	All

Brief outline of proposed new or amended regulatory activity

This document is aimed at all organisations and businesses that will be affected by the GDPR. The GDPR is due to take force in May 2018 and it is expected that organisations will prepare to comply with the GDPR once it is in force. This document provides good practice guidance to assist organisations in preparing for the implementation of the GDPR. It does not impose any obligations beyond those in the Data Protection Act 1998 (the DPA)/the GDPR.

Which type of business will be affected? How many are estimated to be affected?

This guidance is potentially relevant to all businesses that process personal data, ie. many, if not all businesses. However, businesses are not *required* to read this guidance or to implement its recommendations in order to meet their obligations under the DPA/the GDPR, because it does not impose obligations on businesses, beyond what is in legislation. We have therefore based our estimate of the number of businesses affected on an estimate of the number who have accessed the guidance via our website. This produces an estimate of 948 businesses.

Summary of costs and benefits						
Price base year	Implementation date	Duration of policy (years)	Net Present Value	Business Net Present Value	Net cost to business (EANDCB)	BIT score
2014	2016	5	0	0	0	0

Please set out the impact to business clearly with a breakdown of costs and benefits

This document makes recommendations but it does not require business to do anything, beyond the requirements in legislation. We determine therefore that as the guidance allows businesses to act, that it is permissive in nature. It is therefore not possible to estimate in any meaningful way the cost/ benefit to business of taking any action as a result of reading our guidance. There is currently no further evidence available of the cost to business and we believe that it would be disproportionate to attempt to collect further evidence.

It is only possible to estimate the cost of reading the document itself. We therefore consider the impact to business to be the cost of reading the guidance. We believe this approach to be consistent with the document *Draft appraisal of guidance* published by BEIS on the Alfresco collaboration site.

Using the Standard Cost Model, we have calculated the cost of reading the document as follows:

We calculated the Estimated Time to Read (ETTR) the document, by obtaining the Fleisch Reading Ease (FRE) score (using the spelling/ grammar checker in MS Word) and using this to obtain the number of words per minute (using the table in *Draft appraisal of guidance*). Our guidance documents typically fall within the FRE range 30-70; we have taken FRE 30-50 as equivalent to 75 wpm, FRE 50-60 as equivalent to 100 wpm and 60-70 as equivalent to 200 wpm. We then multiplied the wpm by the word count to obtain the ETTR in minutes.

In order to estimate the number of businesses reading the guidance, we took the number of unique page views on our website in 2016 from our own web analytics. To estimate what proportion of website views came from users within businesses, we used the results of a recent ICO website survey. Between 26 May and 9 June 2016, the ICO ran a website user survey, published on the ICO website and publicised through social media channels. During this period, the ICO received 1,741 survey responses, identifying that 48% of users were from organisations and 23.7% of users were from private sector organisations. We therefore multiplied the number of unique page views by 23.7% to determine the number of views from businesses.

We have no way of knowing who within a business is reading our documents and so we have assumed that the typical reader is a manager. We have used the mean hourly wage cost for a manager from the Annual Survey of Hours and Earnings (ASHE) of £24.81 and added 20.2% of the wage cost for on-costs. This 20.2% figure is based upon the latest Eurostat figures, which outlines that non-wage cost, as a proportion of total wage cost is 16.8%. This implies that wage costs are 83.2% of total labour cost. As outlined in the BIT

Assessments: models and data sources document, to calculate the wage + non-wage costs, we multiply the wage cost by $(1 + \text{non-wage cost/wage cost})$. Based on the figure of 16.8%, this works out as $\text{Wage cost} * (1 + (0.168/0.832))$ or $\text{Wage cost} * (1 + 0.202)$.

This gives us the hourly employment cost of a typical reader of our guidance. We have further assumed that this person reads the document once each year, for familiarisation.

In summary, the cost to business of reading the guidance in any one year is therefore:

$$\text{ETTR} \times \text{no. of businesses reading it} \times (\text{wage cost} + \text{on-cost})$$

This gives a figure of £13,668 per annum as the cost to business. The attached spreadsheet sets out the calculation in detail.

We do not believe there is a reliable way to monetise the direct benefit to business of reading our guidance. This is because it is not possible to estimate the counterfactual ie the cost to business of *not* reading our guidance. It may be assumed that, without the guidance, some businesses would pay for legal advice on the points it covers, while others may obtain advice informally from their peers, or internally eg from their data protection officer (if they have one), or simply work out for themselves what to do. The *Draft appraisal of guidance* document contains some estimates of the cost of external advice, but there is no robust way to relate this to advice on the specific points covered by the guidance. As reading the guidance is voluntary, we consider that it is reasonable to expect that business will therefore read it only where it leads to net benefits; the analysis therefore assumes that the benefits are at least equal to the costs.

For the purposes of calculating the EANDCB we have assumed policy duration of five years. This is because the guidance reflects the requirements in the period of transition from DPA to GDPR, and there is also some uncertainty as regards the long term position post- Brexit. It is reasonable to assume that we may revise the guidance after five years, if not before.

Please provide any additional information (if required) that may assist the RPC to validate the BIT Score

Regulator Assessment: Qualifying Regulatory Provisions

Title of proposal	How to disclose information safely – removing personal data from information requests and datasets
Lead Regulator	Information Commissioner's Office (ICO)
Contact for enquiries	Carl Wiper, Group Manager, Policy Delivery carl.wiper@ico.org.uk tel 01625 545503

Date of assessment	21 March 2017
Commencement date	1 October 2015
Origin	Domestic
Does this include implementation of a Cutting Red Tape review?	No
Which areas of the UK will be affected?	All

Brief outline of proposed new or amended regulatory activity

This guidance document explains some of the most common inappropriate disclosures seen by the ICO. The Data Protection Act 1998 (the DPA), Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (the EIR) requires organisations and Public Authorities (PA's) to respond appropriately to requests for information received. This document provides good practice advice on how to respond to such requests without inappropriately disclosing personal or other data in error. It does not impose any obligations beyond those in the DPA, FOIA or the EIR.

Which type of business will be affected? How many are estimated to be affected?

This guidance is potentially relevant to all businesses that process personal data, in addition to any businesses that are a Public Authority under FOIA or the EIR. However, businesses are not *required* to read this guidance or to implement its recommendations in order to meet their obligations under the DPA, because it does not impose obligations on businesses, beyond what is in legislation. We have therefore based our estimate of the number of businesses affected on an estimate of the number who have accessed the guidance via our website. This produces an estimate of 858 businesses.

Summary of costs and benefits						
Price base year	Implementation date	Duration of policy (years)	Net Present Value	Business Net Present Value	Net cost to business (EANDCB)	BIT score
2014	2016	5	0	0	0	0

Please set out the impact to business clearly with a breakdown of costs and benefits

This document makes recommendations but it does not require business to do anything, beyond the requirements in legislation. We determine therefore that as the guidance allows businesses to act, that it is permissive in nature. It is therefore not possible to estimate in any meaningful way the cost/ benefit to business of taking any action as a result of reading our guidance. There is currently no further evidence available of the cost to business and we believe that it would be disproportionate to attempt to collect further evidence.

It is only possible to estimate the cost of reading the document itself. We therefore consider the impact to business to be the cost of reading the guidance. We believe this approach to be consistent with the document *Draft appraisal of guidance* published by BEIS on the Alfresco collaboration site.

Using the Standard Cost Model, we have calculated the cost of reading the document as follows:

We calculated the Estimated Time to Read (ETTR) the document, by obtaining the Fleisch Reading Ease (FRE) score (using the spelling/ grammar checker in MS Word) and using this to obtain the number of words per minute (using the table in *Draft appraisal of guidance*). Our guidance documents typically fall within the FRE range 30-70; we have taken FRE 30-50 as equivalent to 75 wpm, FRE 50-60 as equivalent to 100 wpm and 60-70 as equivalent to 200 wpm. We then multiplied the wpm by the word count to obtain the ETTR in minutes.

In order to estimate the number of businesses reading the guidance, we took the number of unique page views on our website in 2016 from our own web analytics. To estimate what proportion of website views came from users within businesses, we used the results of a recent ICO website survey. Between 26 May and 9 June 2016, the ICO ran a website user survey, published on the ICO website and publicised through social media channels. During this period, the ICO received 1,741 survey responses, identifying that 48% of users were from organisations and 23.7% of users were from private sector organisations. We therefore multiplied the number of unique page views by 23.7% to determine the number of views from businesses.

We have no way of knowing who within a business is reading our documents and so we have assumed that the typical reader is a manager. We have used the mean hourly wage cost for a manager from the Annual Survey of Hours and Earnings (ASHE) of £24.81 and added 20.2% of the wage cost for on-costs. This 20.2% figure is based upon the latest Eurostat figures, which outlines that non-wage cost, as a proportion of total wage cost is 16.8%. This implies that wage costs are 83.2% of total labour cost. As outlined in the BIT assessments: models and data sources document, to calculate the wage + non-wage costs, we multiply the wage cost by $(1 + \text{non-wage cost} / \text{wage cost})$. Based on the figure of

16.8%, this works out as Wage cost * (1+(0.168/0.832)) or Wage cost * (1+0.202).

This gives us the hourly employment cost of a typical reader of our guidance. We have further assumed that this person reads the document once each year, for familiarisation.

In summary, the cost to business of reading the guidance in any one year is therefore:

$$\text{ETTR} \times \text{no. of businesses reading it} \times (\text{wage cost} + \text{on-cost})$$

This gives a figure of £39,252 per annum as the cost to business. The attached spreadsheet sets out the calculation in detail.

We do not believe there is a reliable way to monetise the direct benefit to business of reading our guidance. This is because it is not possible to estimate the counterfactual ie the cost to business of *not* reading our guidance. It may be assumed that, without the guidance, some businesses would pay for legal advice on the points it covers, while others may obtain advice informally from their peers, or internally eg from their data protection officer (if they have one), or simply work out for themselves what to do. The *Draft appraisal of guidance* document contains some estimates of the cost of external advice, but there is no robust way to relate this to advice on the specific points covered by the guidance. As reading the guidance is voluntary, based on the reasonable expectation that business will read the guidance only where it leads to net benefits, the analysis assumes that the benefits are at least equal to the costs.

For the purposes of calculating the EANDCB we have assumed policy duration of five years. This is because the guidance reflects the requirements in the period of transition from DPA to GDPR, and there is also some uncertainty as regards the long term position post- Brexit. It is reasonable to assume that we may revise the guidance after five years, if not before.

Please provide any additional information (if required) that may assist the RPC to validate the BIT Score

Regulator Assessment: Qualifying Regulatory Provisions

Title of proposal	Assessing Adequacy – International Data Transfers
Lead Regulator	Information Commissioner's Office (ICO)
Contact for enquiries	Carl Wiper, Group Manager, Policy Delivery carl.wiper@ico.org.uk tel 01625 545503

Date of assessment	21 March 2017
Commencement date	29 September 2015
Origin	Domestic
Does this include implementation of a Cutting Red Tape review?	No
Which areas of the UK will be affected?	All

Brief outline of proposed new or amended regulatory activity

This guidance document explains how organisations should carry out assessments of the adequacy of protection available in respect of a proposed transfer of personal data outside of the European Economic Area (the EEA).

The Data Protection Act 1998 (the DPA) provides that personal data shall not be transferred to a country or territory outside of the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjected in relation to the processing of personal data. This document provides good practice advice on how to meet this requirement. It does not impose any obligations beyond those in the DPA.

Which type of business will be affected? How many are estimated to be affected?

This guidance is potentially relevant to all businesses that process personal data, especially where such processing requires a transfer of data to another territory. However, businesses are not *required* to read this guidance or to implement its recommendations in order to meet their obligations under the DPA, because it does not impose obligations on businesses, beyond what is in legislation. We have therefore based our estimate of the number of businesses affected on an estimate of the number who have accessed the guidance via our website. This produces an estimate of 903 businesses.

Summary of costs and benefits						
Price base year	Implementation date	Duration of policy (years)	Net Present Value	Business Net Present Value	Net cost to business (EANDCB)	BIT score
2014	2016	5	0	0	0	0

Please set out the impact to business clearly with a breakdown of costs and benefits

This document makes recommendations but it does not require business to do anything, beyond the requirements in legislation. We determine therefore that as the guidance allows businesses to act, that it is permissive in nature. It is therefore not possible to estimate in any meaningful way the cost/ benefit to business of taking any action as a result of reading our guidance. There is currently no further evidence available of the cost to business and we believe that it would be disproportionate to attempt to collect further evidence.

It is only possible to estimate the cost of reading the document itself. We therefore consider the impact to business to be the cost of reading the guidance. We believe this approach to be consistent with the document *Draft appraisal of guidance* published by BEIS on the Alfresco collaboration site.

Using the Standard Cost Model, we have calculated the cost of reading the code as follows:

We calculated the Estimated Time to Read (ETTR) the document, by obtaining the Fleisch Reading Ease (FRE) score (using the spelling/ grammar checker in MS Word) and using this to obtain the number of words per minute (using the table in *Draft appraisal of guidance*). Our guidance documents typically fall within the FRE range 30-70; we have taken FRE 30-50 as equivalent to 75 wpm, FRE 50-60 as equivalent to 100 wpm and 60-70 as equivalent to 200 wpm. We then multiplied the wpm by the word count to obtain the ETTR in minutes.

In order to estimate the number of businesses reading the guidance, we took the number of unique page views on our website in 2016 from our own web analytics. To estimate what proportion of website views came from users within businesses, we used the results of a recent ICO website survey. Between 26 May and 9 June 2016, the ICO ran a website user survey, published on the ICO website and publicised through social media channels. During this period, the ICO received 1,741 survey responses, identifying that 48% of users were from organisations and 23.7% of users were from private sector organisations. We therefore multiplied the number of unique page views by 23.7% to determine the number of views from businesses.

We have no way of knowing who within a business is reading our documents and so we have assumed that the typical reader is a manager. We have used the mean hourly wage cost for a manager from the Annual Survey of Hours and Earnings (ASHE) of £24.81 and added 20.2% of the wage cost for on-costs. This 20.2% figure is based upon the latest Eurostat figures, which outlines that non-wage cost, as a proportion of total wage cost is 16.8%. This implies that wage costs are 83.2% of total labour cost. As outlined in the BIT

assessments: models and data sources document, to calculate the wage + non-wage costs, we multiply the wage cost by $(1 + \text{non-wage cost/wage cost})$. Based on the figure of 16.8%, this works out as $\text{Wage cost} * (1 + (0.168/0.832))$ or $\text{Wage cost} * (1 + 0.202)$.

This gives us the hourly employment cost of a typical reader of our guidance. We have further assumed that this person reads the document once each year, for familiarisation.

In summary, the cost to business of reading the guidance in any one year is therefore:

$$\text{ETTR} \times \text{no. of businesses reading it} \times (\text{wage cost} + \text{on-cost})$$

This gives a figure of £10,774 per annum as the cost to business. The attached spreadsheet sets out the calculation in detail.

We do not believe there is a reliable way to monetise the direct benefit to business of reading our guidance. This is because it is not possible to estimate the counterfactual ie. the cost to business of *not* reading our guidance. It may be assumed that, without the guidance, some businesses would pay for legal advice on the points it covers, while others may obtain advice informally from their peers, or internally eg from their data protection officer (if they have one), or simply work out for themselves what to do. The *Draft appraisal of guidance* document contains some estimates of the cost of external advice, but there is no robust way to relate this to advice on the specific points covered by the guidance. As reading the guidance is voluntary based on the reasonable expectation that business will read the guidance only where it leads to net benefits, the analysis assumes that the benefits are at least equal to the costs.

For the purposes of calculating the EANDCB we have assumed policy duration of five years. This is because the guidance reflects the requirements in the period of transition from DPA to GDPR, and there is also some uncertainty as regards the long term position post- Brexit. It is reasonable to assume that we may revise the guidance after five years, if not before.

Please provide any additional information (if required) that may assist the RPC to validate the BIT Score

Regulator Assessment: Qualifying Regulatory Provisions

Title of proposal	Privacy Notices Code of Practice
Lead Regulator	Information Commissioner's Office (ICO)
Contact for enquiries	Carl Wiper, Group Manager, Policy Delivery carl.wiper@ico.org.uk tel 01625 545503

Date of assessment	21 March 2017
Commencement date	7 October 2016
Origin	Domestic and European Union (EU)
Does this include implementation of a Cutting Red Tape review?	No
Which areas of the UK will be affected?	All

Brief outline of proposed new or amended regulatory activity

This is a Code of Practice issued by the Information Commissioner under section 51 of the Data Protection Act 1998 (the DPA). This requires her to promote good practice, including compliance with the DPA's requirements, and empowers her, after consultation, to prepare codes of practice giving guidance on good practice.

The basic legal requirement is to comply with the DPA itself. Organisations may use alternative methods to meet the DPA's requirements, but if they do nothing then they risk breaking the law. The Information Commissioner cannot take action over a failure to adopt good practice or to act on the recommendations set out in the code. However, she can pursue enforcement action where an organisation breaches the requirements of the DPA. Furthermore, when considering whether or not the DPA has been breached the Information Commissioner can have due regard to the advice provided in this document.

This Code of Practice provides advice, guidance and good practice recommendations to organisations, including businesses, to help them to meet their obligations to tell people how they are using their personal data and to seek consent where appropriate. These obligations arise from the current DPA and are further developed in the new EU General Data Protection Regulation. The document covers the requirements of both the DPA and the GDPR.

Which type of business will be affected? How many are estimated to be affected?

This Code of Practice is potentially relevant to all businesses that process personal data, ie most if not all businesses in the country. However, businesses are not *required* to read this Code or to implement its recommendations in order to meet their obligations under the DPA or the GDPR, because it does not impose obligations on businesses, beyond what is in legislation. We have therefore based our estimate of the number of businesses affected on an estimate of the number who have accessed the Code via our website. This produces an estimate of 8840 businesses.

Summary of costs and benefits

Price base year	Implementation date	Duration of policy (years)	Net Present Value	Business Net Present Value	Net cost to business (EANDCB)	BIT score
2014	2016	5	0	0	0	0

Please set out the impact to business clearly with a breakdown of costs and benefits

This document makes recommendations but it does not require business to do anything, beyond the requirements in legislation. We determine therefore that as the Code allows businesses to act, that it is permissive in nature. It is therefore not possible to estimate in any meaningful way the cost/ benefit to business of taking any action as a result of reading the Code. There is currently no further evidence available of the cost to business and we believe that it would be disproportionate to attempt to collect further evidence.

It is only possible to estimate the cost of reading the document itself. We therefore consider the impact to business to be the cost of reading the Code. We believe this approach to be consistent with the document *Draft appraisal of guidance* published by BEIS on the Alfresco collaboration site.

Using the Standard Cost Model, we have calculated the cost of reading the code as follows:

We calculated the Estimated Time to Read (ETTR) the document, by obtaining the Fleisch Reading Ease (FRE) score (using the spelling/ grammar checker in MS Word) and using this to obtain the number of words per minute (using the table in *Draft appraisal of guidance*). Our guidance documents typically fall within the FRE range 30-70; we have taken FRE 30-50 as equivalent to 75 wpm, FRE 50-60 as equivalent to 100 wpm and 60-70 as equivalent to 200 wpm. We then multiplied the wpm by the word count to obtain the ETTR in minutes.

In order to estimate the number of businesses reading the Code, we took the number of unique page views on our website in 2016 from our own web analytics. To estimate what proportion of website views came from users within businesses, we used the results of a recent ICO website survey. Between 26 May and 9 June 2016, the ICO ran a website user survey, published on the ICO website and publicised through social media channels. During this period, the ICO received 1,741 survey responses, identifying that 48% of

users were from organisations and 23.7% of users were from private sector organisations. We therefore multiplied the number of unique page views by 23.7% to determine the number of views from businesses.

We have no way of knowing who within a business is reading our documents and so we have assumed that the typical reader is a manager. We have used the mean hourly wage cost for a manager from the Annual Survey of Hours and Earnings (ASHE) of £24.81 and added 20.2% of the wage cost for on-costs. This 20.2% figure is based upon the latest Eurostat figures, which outlines that non-wage cost, as a proportion of total wage cost is 16.8%. This implies that wage costs are 83.2% of total labour cost. As outlined in the BIT assessments: models and data sources document, to calculate the wage + non-wage costs, we multiply the wage cost by $(1 + \text{non-wage cost}/\text{wage cost})$. Based on the figure of 16.8%, this works out as $\text{Wage cost} * (1 + (0.168/0.832))$ or $\text{Wage cost} * (1 + 0.202)$.

This gives us the hourly employment cost of a typical reader of the Code. We have further assumed that this person reads the document once each year, for familiarisation.

In summary, the cost to business of reading the Code in any one year is therefore:

$$\text{ETTR} \times \text{no. of businesses reading it} \times (\text{wage cost} + \text{on-cost})$$

This gives a figure of £608,241 per annum as the cost to business. The attached spreadsheet sets out the calculation in detail.

We do not believe there is a reliable way to monetise the direct benefit to business of reading the Code. This is because it is not possible to estimate the counterfactual ie the cost to business of *not* reading the Code. It may be assumed that, without the Code, some businesses would pay for legal advice on the points it covers, while others may obtain advice informally from their peers, or internally eg from their data protection officer (if they have one), or simply work out for themselves what to do. The *Draft appraisal of guidance* document contains some estimates of the cost of external advice, but there is no robust way to relate this to advice on the specific points covered by the Code. As reading the Code is voluntary, we consider that it is reasonable to expect that business will therefore read it only where it leads to net benefits; the analysis therefore assumes that the benefits are at least equal to the costs.

For the purposes of calculating the EANDCB we have assumed policy duration of five years. This is because the Code reflects the requirements in the period of transition from DPA to GDPR, and there is also some uncertainty as regards the long term position post-Brexit. It is reasonable to assume that we may revise the Code after five years, if not before.

Please provide any additional information (if required) that may assist the RPC to validate the BIT Score

Regulator Assessment: Qualifying Regulatory Provisions

Title of proposal	Overview of the GDPR
Lead Regulator	Information Commissioner's Office (ICO)
Contact for enquiries	Carl Wiper, Group Manager, Policy Delivery carl.wiper@ico.org.uk tel 01625 545503

Date of assessment	21 March 2017
Commencement date	7 July 2016
Origin	European Union (EU)
Does this include implementation of a Cutting Red Tape review?	No
Which areas of the UK will be affected?	All

Brief outline of proposed new or amended regulatory activity

This document provides advice and guidance on the provisions of the General Data Protection Regulations (the GDPR). The GDPR sets out a new legal framework for the processing of personal data in the EU. This document provides organisation with advice on how to comply with this framework. It does not impose any obligations beyond those in the DPA/the GDPR.

Which type of business will be affected? How many are estimated to be affected?

This guidance is potentially relevant to all businesses that process personal data, ie most if not all businesses. However, businesses are not *required* to read this guidance or to implement its recommendations in order to meet their obligations under the DPA/the GDPR, because it does not impose obligations on businesses, beyond what is in legislation. We have therefore based our estimate of the number of businesses affected on an estimate of the number who have accessed the guidance via our website. This produces an estimate of 50763 businesses.

Summary of costs and benefits						
Price base year	Implementation date	Duration of policy (years)	Net Present Value	Business Net Present Value	Net cost to business (EANDCB)	BIT score
2014	2016	5	0	0	0	0

Please set out the impact to business clearly with a breakdown of costs and benefits

This document makes recommendations but it does not require business to do anything, beyond the requirements in legislation. We determine therefore that as the guidance allows businesses to act, that it is permissive in nature. It is therefore not possible to estimate in any meaningful way the cost/ benefit to business of taking any action as a result of reading our guidance. There is currently no further evidence available of the cost to business and we believe that it would be disproportionate to attempt to collect further evidence.

It is only possible to estimate the cost of reading the document itself. We therefore consider the impact to business to be the cost of reading the guidance. We believe this approach to be consistent with the document *Draft appraisal of guidance* published by BEIS on the Alfresco collaboration site.

Using the Standard Cost Model, we have calculated the cost of reading the document as follows:

We calculated the Estimated Time to Read (ETTR) the document, by obtaining the Fleisch Reading Ease (FRE) score (using the spelling/ grammar checker in MS Word) and using this to obtain the number of words per minute (using the table in *Draft appraisal of guidance*). Our guidance documents typically fall within the FRE range 30-70; we have taken FRE 30-50 as equivalent to 75 wpm, FRE 50-60 as equivalent to 100 wpm and 60-70 as equivalent to 200 wpm. We then multiplied the wpm by the word count to obtain the ETTR in minutes.

In order to estimate the number of businesses reading the guidance, we took the number of unique page views on our website in 2016 from our own web analytics. To estimate what proportion of website views came from users within businesses, we used the results of a recent ICO website survey. Between 26 May and 9 June 2016, the ICO ran a website user survey, published on the ICO website and publicised through social media channels. During this period, the ICO received 1,741 survey responses, identifying that 48% of users were from organisations and 23.7% of users were from private sector organisations. We therefore multiplied the number of unique page views by 23.7% to determine the number of views from businesses.

We have no way of knowing who within a business is reading our documents and so we have assumed that the typical reader is a manager. We have used the mean hourly wage cost for a manager from the Annual Survey of Hours and Earnings (ASHE) of £24.81 and added 20.2% of the wage cost for on-costs. This 20.2% figure is based upon the latest Eurostat figures, which outlines that non-wage cost, as a proportion of total wage cost is 16.8%. This implies that wage costs are 83.2% of total labour cost. As outlined in the BIT

assessments: models and data sources document, to calculate the wage + non-wage costs, we multiply the wage cost by $(1 + \text{non-wage cost/wage cost})$. Based on the figure of 16.8%, this works out as $\text{Wage cost} * (1 + (0.168/0.832))$ or $\text{Wage cost} * (1 + 0.202)$.

This gives us the hourly employment cost of a typical reader of our guidance. We have further assumed that this person reads the document once each year, for familiarisation.

In summary, the cost to business of reading the guidance in any one year is therefore:

$$\text{ETTR} \times \text{no. of businesses reading it} \times (\text{wage cost} + \text{on-cost})$$

This gives a figure of £3,481,806 per annum as the cost to business. The attached spreadsheet sets out the calculation in detail.

We do not believe there is a reliable way to monetise the direct benefit to business of reading our guidance. This is because it is not possible to estimate the counterfactual ie the cost to business of *not* reading our guidance. It may be assumed that, without the guidance, some businesses would pay for legal advice on the points it covers, while others may obtain advice informally from their peers, or internally eg from their data protection officer (if they have one), or simply work out for themselves what to do. The *Draft appraisal of guidance* document contains some estimates of the cost of external advice, but there is no robust way to relate this to advice on the specific points covered by the guidance. As reading the guidance is voluntary, based on the reasonable expectation that business will read the guidance only where it leads to net benefits, the analysis assumes that the benefits are at least equal to the costs.

For the purposes of calculating the EANDCB we have assumed policy duration of five years. This is because the guidance reflects the requirements in the period of transition from DPA to GDPR, and there is also some uncertainty as regards the long term position post- Brexit. It is reasonable to assume that we may revise the guidance after five years, if not before.

Please provide any additional information (if required) that may assist the RPC to validate the BIT Score