



Department for
Science, Innovation,
& Technology

Survey of App Developers: Technical Report

Final report

February 2024

Contents

Methodology.....	3
Mapping exercise and sampling	3
Survey of app developers	8
Achieved sample and weighting	9
In-depth interviews	10
Analysis and statistical testing	12
Strengths and limitations of the survey overall	13
Survey questionnaire.....	15
Interview topic guide	29

Methodology

The research comprised three core methodological strands.

- Mapping exercise
- Survey of 600 app developers
- Follow-up depth interviews with 20 app developers

This report sets out further detail on the methodological approach and rationale and should be read alongside the main report.

Mapping exercise and sampling

The purpose of this was to explore the detail and extent of data available relating to the population of app developers in the UK, to inform the sampling approach to the survey fieldwork.

The app development industry as we think of it today is one which has only emerged in recent years and is expanding rapidly. However, while there is no definition of what is meant by an 'app' in the Code of Practice, the fundamentals of computer programming which underpin app development are well-established. Apps generally (but not exclusively) tend to be for specific purposes and many companies which develop apps overlap with traditional software developers (who may also themselves work across different types of software).

As outlined below, there is little available information on the size and scale of the population of app developers. Without an accurate understanding of the population, it is difficult to be able to derive definitive sampling targets. Furthermore, app developers cannot easily be categorised in any Standard Industrial Classification (SIC) codes, and there is very little information available on the firmographic profile of app developers operating in the UK.

Therefore, while the primary research aim was to understand awareness and impact of the Code of Practice introduced in December 2022, a secondary aim was to understand more clearly the make-up of the app developer population.

While app developers do not clearly fall into one SIC code, two were identified as being the most likely and relevant to app developer businesses. These SIC codes could therefore be used as a proxy from which the app developer population could be estimated, and approximate sampling targets derived.

- 6201 computer programming activities (inc. 6201/2 Business and domestic software development).
- 6202 computer consultancy.

Of these two codes, it appeared that 6201 was the most relevant and that 6202, while relevant, was so to a lesser extent.¹

Relevant national datasets were explored to estimate the population of app developers in the UK, both overall and by size and by region. Sources examined include NOMIS (UK Business

¹ See <http://www.siccodesupport.co.uk/sic-division.php?division=62> for further information.

counts) and ONS published data (business population estimates; business demography statistics; business survey and employment register) which helped provide an indication of the number of businesses and breakdown by size/region in these SIC codes.

A variety of secondary sources were examined including freely available reports such as IBISWorld's 2023 report,² statistical releases, and supplemented by key word searches. This provided an idea of total number of app developers in the UK.

Secondary sources were examined for any information on the population profile beyond region/size (for instance, number of app developers by platform) but little to no data were publicly available.

Estimating the population profile of UK app developers

A stratified random sampling approach was adopted using the UK business populations for SIC codes 6201 and 6202. Using the ONS/Nomis dataset Business Counts 2022, data relating to the number of businesses in SIC codes 6201 and 6202 by size and by region were obtained. Findings are outlined in the tables below.

Table 1 Number of businesses in SIC code 6201 by region and by size

Total 6201	Total	Micro (0 to 9)	Small (10 to 49)	Medium (50 to 249)	Large (250+)
East of England	2,780	2,540	200	35	5
East Midlands	1,400	1,255	105	35	0
London	9,985	8,825	920	215	25
North East	585	525	50	10	0
North West	2,420	2,160	220	40	5
South East	5,815	5,210	485	95	20
South West	2,405	2,170	195	40	0
West Midlands	1,835	1,660	135	30	10
Yorkshire and The Humber	1,530	1,370	130	20	5
Northern Ireland	585	505	60	15	5
Scotland	1,430	1,250	155	20	5
Wales	710	650	50	10	0
Total	31,485	28,125	2,700	575	85

² IBISWorld (2023) [App Development in the UK - Market Research Report](#)

Table 2 Number of businesses in SIC code 6202 by region and by size

Total 6202	Total	Micro (0 to 9)	Small (10 to 49)	Medium (50 to 249)	Large (250+)
East of England	8,700	8,385	270	35	10
East Midlands	4,135	3,935	175	20	0
London	24,575	23,495	850	190	40
North East	1,275	1,215	50	10	5
North West	5,795	5,540	200	50	5
South East	18,640	17,760	710	135	35
South West	5,895	5,645	215	30	0
West Midlands	5,400	5,155	200	40	5
Yorkshire and The Humber	3,930	3,720	175	30	5
Northern Ireland	720	680	30	5	5
Scotland	3,520	3,380	105	35	5
Wales	1,580	1,510	60	10	0
Total	84,160	80,425	3,040	585	110

Sources such as IBISWorld’s 2023 report,³ the National Cyber Security Centre’s 2022 report,⁴ and information available from 42Matters⁵ respectively suggest there are – in total – 13,340, over 10,000, and 10,787 app developers based in the UK – all figures that are roughly in a similar order of magnitude. Further information on the spread of such businesses by size or region is not readily available.

However, using this as a starting point, and assuming that all app developers fall into either the 6201 or 6202 SIC codes, an estimate of the profile of UK app developers by size and by region can be made.

As noted as part of the mapping exercise findings above, the most relevant SIC code is 6201, and 6202 is somewhat relevant, albeit to a lesser extent. Greater weighting was therefore placed on 6201 over 6202, with a 70:30 split in calculating population estimates and sampling targets to ensure greater emphasis was placed on businesses in 6201.

To do this, the proportion of app developers relative to the total number of 6201 and 6202 businesses was calculated, assuming that 70% of app developers fall into 6201, and 30% into 6202.

Taking the IBIS report figure of 13,340 and splitting this 70:30 gave 9,340 app developers in 6201 and 4,000 in 6202.

Then, taking these figures and dividing them by the total number of businesses in 6201 and 6202, respectively, gave the proportion of app developers in each SIC code.

- For 6201: $9,340/31,485 = 29.7\%$ of businesses in 6201 are app developers.
- For 6202: $4,000/84,160 = 4.8\%$ of businesses in 6202 are app developers.

These respective proportions can then be applied to the two tables above, and the totals summed together, to determine an estimate of the profile of app developers in the UK. This

³ IBISWorld (2023) [App Development in the UK - Market Research Report](#)

⁴ National Cyber Security Centre (2022) [Threat report on application stores](#), p6

⁵ 42Matters (2023) [How Many Mobile App Developers Are From the United Kingdom?](#)

assumes that the 70:30 split is applicable consistently across app developers by region and by size. This is shown in the table below, with outputs rounded to the nearest five.

Table 3 Estimated profile of app developers in the UK

Estimated number of app developers in the UK	Total	Micro (0 to 9)	Small (10 to 49)	Medium (50 to 249)	Large (250+)
East of England	1,240	1,150	70	10	0
East Midlands	610	560	40	10	0
London	4,130	3,735	315	75	10
North East	235	215	15	5	0
North West	995	905	75	15	0
South East	2,610	2,390	180	35	10
South West	995	910	70	15	0
West Midlands	800	735	50	10	5
Yorkshire and The Humber	640	585	45	5	0
Northern Ireland	210	180	20	5	0
Scotland	590	530	50	10	0
Wales	285	265	20	5	0
Total	13,340	12,160	950	200	25

Note that it was outside of the project scope to undertake a similar mapping exercise of app developers based overseas. Details on the sampling strategy in relation to app developers based outside of the UK is contained in the following section.

Sampling strategy

Based on using SIC codes as a proxy for the UK app developer population, an initial sample could be developed for the survey of 600 app developers.

Prior to undertaking the mapping exercise, it was envisaged that the fieldwork would engage with the following groups.

- 550 app developers based in the UK and 50 overseas.
- In the UK, with at least 50 app developers per size band.

Calculations to estimate the number of app developers in the UK suggested that there were only around 25 large app developers in the UK, and 200 medium sized businesses. This meant that the initial target of 50 completions for each size band was adjusted downward to speak to up to 10 large companies and 40 medium businesses.

Table 4 Preliminary sample targets by company size (UK)

Size-band	Sample size (min)	% of sample
UK target	550	100%
Micro (1 to 9 employees)	275	50%
Small (10 to 49 employees)	225	41%
Medium (50 to 249 employees)	40	7%
Large (250+ employees)	10	2%

Representative sample targets by region/nation could also be determined using the information derived from SIC codes to calculate an estimated profile of UK app developers.

Table 5 Preliminary sample targets by region (UK)

Region	Total businesses	Representative sample
East of England	1,240	50
East Midlands	610	25
London	4,130	170
North East	235	10
North West	995	40
South East	2,610	110
South West	995	40
West Midlands	800	35
Yorkshire and The Humber	640	25
Northern Ireland	210	10
Scotland	590	25
Wales	285	10
Total	13,340	550

For app developers based abroad, nations to be targeted were agreed with DSIT and included the USA, western Europe and key Asian countries. Due to the tight fieldwork timeline, and the protracted nature of reaching some countries with significant time zone differences, the bulk of the overseas completions were targeted at app developers based in western Europe.

As detailed in the mapping exercise findings (above), existing sources were examined to understand the extent and nature of any further information relating to the profile of the UK app developer population, for example by platform, to further inform the sampling by additional criteria. However, such data were not freely available and detailed granular information in this regard was not publicly available, despite extensive searching.

For this reason, preliminary quotas were not set for any other parameters except by size and region.

However, bearing in mind that there was very limited data available on the size and scale of the UK app developer population, the research used the above sampling targets – derived from using the two SIC codes as a proxy – as approximate guiding targets for the fieldwork.

Given that an additional intention of the research was to further understand the UK app developer population, it was important that these targets were used as a guide only. Further, it was important that a random approach was taken to engaging with app developers that would result in an achieved sample that was representative of the UK app developer population. In other words, the targets derived from using SIC codes as a proxy were used as a rough guide only and were not beholden to, and the achieved sample was allowed to fall out 'naturally' as part of the fieldwork and contact/engagement with app developers.

Alongside this, it was important that feedback was obtained from a wide range of app developers (by size, region, platform) and therefore completions were closely monitored during fieldwork to ensure that a spread of responses was indeed being achieved through this random approach.

Survey of app developers

Pilot

The survey questionnaire was initially piloted using Computer Assisted Telephone Interviewing (CATI). For this piloting stage, the questions were appended with a series of feedback questions to gather respondents' views on the clarity and ease of participation. In the main, the survey was found to be clear and easy to understand.

However, on the back of feedback from initial interviews, some changes were made.

- The scope was clarified to not include web designers who incorporate apps in their websites (however, some completions were achieved with some app developers who develop apps for platforms in scope as well as developing apps for websites).
- Some layman definitions for questions that were felt to include more technical language were added as footnotes if clarification was requested by the interviewer.
- The question around costs was too granular for respondents to be able to answer, so this was simplified to ask about fewer elements at a higher level. This section was also split so that those aware of the Code were routed to be asked about costs associated with implementing the Code, while those unaware of the Code were routed to be asked about costs associated with implementing a voluntary set of security and privacy guidelines. Pilot feedback suggested respondents unaware of the Code felt unable to provide cost information about the Code when they were unaware of it, but were able to provide some high-level information about a set of guidelines. This approach was therefore taken to be able to gather some high-level cost information.

Once changes were implemented, the full fieldwork went live using a mixed-method approach of CATI and online. The finalised questionnaire can be found below.

Survey promotion

The research was promoted by DSIT on the gov.uk website.

Further, a letter of endorsement signed by a senior DSIT official was circulated to several industry bodies to raise awareness of the research, who were asked to promote the research among their member organisations. App developers could either respond online or register interest in a call-back.

Contacts

Bureau van Dijk's FAME database was used to obtain contact details of companies that were potentially in scope of the research. This was supplemented with details of potential app developers obtained from MarketScan, as well as freely available online sources and databases of app developer companies. Contacts from different sources were merged and de-duplicated prior to engagement.

A random approach was taken to engagement, meaning that there was no pre-determined approach to which developers would be contacted, nor in which order. Contacts were arranged into a random order and interviewers worked through their contact list from top to bottom, thus ensuring that a random approach was taken.

A sizeable proportion of contacts obtained were out of scope of the study, were unavailable to participate at the time fieldwork was live, or were unable to be directly contacted. To maximise participation, companies were called back at different times and days of the week, and appointments were offered out of hours as necessary.

Despite the challenges of engagement, the full survey target was reached. Further, given the combination of the mapping exercise that was undertaken to derive the sampling targets using SIC codes as a proxy, and the approach taken to engagement, the achieved sample can be said to be representative of the UK app developer population.

Achieved sample and weighting

Completions were closely monitored during fieldwork to ensure that a spread of responses (by size, region, platform) was achieved through a random approach but this did not fundamentally impact or skew the final sample that was obtained.

The tables below illustrate the target and actual samples achieved.

Table 6 Target and achieved samples by size

Size-band	Target sample	Achieved sample	Achieved/target %
Micro (one to nine employees)	275	420	153%
Small (10 to 49 employees)	225	159	71%
Medium (50 to 249 employees)	40	15	38%
Large (250+ employees)	10	6	60%

Table 7 Target and achieved samples by region

Region	Target sample	Achieved sample	Achieved/target %
East of England	50	37	74%
East Midlands	25	35	140%
London	170	117	69%
North East	10	13	130%
North West	40	43	108%
South East	110	96	87%
South West	40	63	158%
West Midlands	35	50	143%
Yorkshire and The Humber	25	33	132%
Northern Ireland	10	8	80%
Scotland	25	30	120%
Wales	10	14	140%
Total	550	539	-

The achieved sample indicates a strong skew towards micro and small companies, as was initially suggested through the exercise to estimate the UK app developer population, and is typical of the ‘normal’ structure of sector business populations. As a reminder, this proxy was based on size and region sample targets derived from SIC data for the two main relevant SIC codes.

The survey data were not weighted prior to analysis.

In the right situation, weighting can be a useful tool. However, if not used extremely carefully, it can also distort the picture and result in misleading figures. Weighting of data depends fundamentally on an accurate understanding of the population and should be used with caution. To be able to employ weighting accurately, it is necessary to know the precise characteristics of the population. Existing official statistics and the limited information contained in other reports provided little assistance in identifying elements of the population.

Therefore, given that the achieved sample mirrors the ‘normal’ structure of sector business populations, and that only limited insight into the distribution of the UK app developer population could be obtained from the initial mapping exercise, weighting was not applied.

However, this exercise – a first of its kind – has provided invaluable information on the size and scale of the UK app developer population and will be a useful benchmark and consideration for deriving sample targets for any future studies with app developers.

In-depth interviews

The qualitative strand of the research aimed to build on survey responses to understand how and why developers use their current processes, and how the Code would impact their businesses and practices. A topic guide was designed jointly between Pye Tait Consulting and DSIT, and a copy is available below.

Surveyed app developers had the opportunity, at the end of the survey, to register interest in a follow-up in-depth interview. From this pool, Pye Tait purposefully drew a sample to achieve 20 interviews in November 2023 with a range of app developers by company size, region, and awareness of the Code prior to participating in the survey.

It was agreed with DSIT that at least 25% of in-depth interviews would be undertaken with those aware of the Code, to ensure that detailed views could be gathered from a group who had some familiarity with it. It was further agreed that interviews would be conducted only with developers based in the UK and that, given the South East and London were the regions with the highest proportions of survey respondents, that a geographic spread should be achieved to ensure a split between South East/London and other parts of the UK.

Pye Tait contacted app developers who had registered interest and who fitted the sample profile to arrange a convenient appointment. In advance of the conversation, interviewees were sent a copy of the Code to familiarise themselves with this. Interviews were conducted virtually over MS Teams or telephone.

The achieved sample profile of the 20 in-depth interview participants is outlined below.

Table 8 Achieved in-depth interview sample by company size

Size	Number of interviews	Percentage of sample
Micro (one to nine employees)	9	45%
Small (10 to 49)	8	40%
Medium (50 to 249)	2	10%
Large (250+)	1	5%
Total	20	100%

Table 9 Achieved in-depth interview sample by region

Region/nation	Number of interviews	Percentage of sample
South East	4	20%
London	3	15%
East Midlands	2	10%
North West	2	10%
South West	2	10%
West Midlands	2	10%
Scotland	2	10%
East of England	1	5%
Yorkshire and the Humber	1	5%
Wales	1	5%
Total	20	100%

Table 10 Achieved in-depth interview sample by prior awareness of the Code

Awareness of the Code	Number of interviews	Percentage of sample
Aware	5	25%
Unaware	15	75%
Total	20	100%

Analysis and statistical testing

Following fieldwork close, all survey data were cleaned. This involved checking for any duplicate submissions from the same app developer, any inconsistencies or outliers, and back-/post-coding any responses as required. Open-ended questions were reviewed to redact any information which might identify individuals or organisations prior to sharing the datafile with DSIT.

A derived variable was created, based on the number of staff directly employed by surveyed app developers, to segment respondents into size categories.

- Fewer than 10 directly employed staff: Micro
- 10 to 49: Small
- 50 to 249: Medium
- 250+: Large

T tests were undertaken to identify any statistically significant differences between the following sub-groups of respondents.

- Company size (number of directly employed staff).
- Region where business headquartered.
- Nation where business headquartered (for app developers based overseas).
- Platform for which apps are developed.
- Whether or not aware of the Code of Practice.

Cross-tabulations were reviewed to ensure sample sizes/cells were of sufficient size to provide meaningful onward analysis and comparison, i.e. that there was a large enough base. Any limitations and interpretations are flagged in the report to readers.

Two confidence intervals were set for testing – 95% and 99%. The word ‘significant’ is used in the report only to identify statistically significant differences at the 95% confidence interval.

Qualitative in-depth interviews were analysed manually. Responses to each question were reviewed, and a coding frame was developed that detailed the key themes. Responses were then coded according to the frame and this was used to identify overall frequency and any noticeable trend by sub-group (e.g. by awareness of the Code, or by platform).

Strengths and limitations of the survey overall

While there have been various reports about app developers in recent years, these have often been lacking in granular information. For example, recent reports have only provided a ballpark estimate of the number of app developers based in the UK, and have not provided further information on the firmographic profile of the population to detail the spread by size or region.

By contrast, this first wave of the app developer survey is intended to be statistically representative of the UK app developer population. Particular strengths of the survey include the following.

- The use of a stratified random sampling approach and interviewing to avoid selection bias.
- The inclusion of app developers of all sizes, from all UK nations and English regions, and who develop apps for different platforms.
- A data collection approach predominantly conducted by telephone which was key to ensuring that a sufficient sample size could be achieved.
- For the first time, gaining an understanding of the level of awareness of the Code among app developers operating in the UK – both spontaneous and prompted – and support required to help align to the principles.
- Gaining a consideration of the financial cost to app developers of implementing the Code.
- This first wave of research with app developers operating in the UK has provided detailed information of the profile of the UK app developer population which can be used as a basis for future reference and research.

At the same time, while the survey aims to produce the most representative, accurate and reliable data possible with the resources available, it should be acknowledged that there are inevitable limitations of the data, as with any survey project. The following might be considered the main limitations.

- A significant challenge is designing a methodology that accurately captures the financial cost of implementing the Code, given that the survey findings necessarily depend on self-reported costs from organisations. Pilot feedback suggested that app developers were unable (or unwilling) to provide costs at a granular level of detail, meaning costs were only queried at a high-level. There is also uncertainty in whether costs provided by app developers relate to short-term costs, or whether these are ongoing, as well as whether such costs are scalable (e.g. by size of business).
- This research predominantly focused on app developers based in the UK, with 61 of the 600 completions from overseas countries, most of which were based in the USA and Western Europe. There will be other app developers in those and other countries who will have a substantial UK market presence. This research engaged with app

developers based overseas, in the most prominent tech countries outside of the UK, to attempt to address this limitation.

- App developers may be inclined to give answers that reflect favourably on them in surveys with government clients, or may be less inclined to take part because of the client, although we have no direct evidence of this. Moreover, we make a concerted effort to overcome this in the administration of the survey by making it clear to respondents that their answers are confidential and reported on anonymously.

Survey questionnaire

App Developers Security and Privacy Practices

Introduction

In 2022, the UK Government published the National Cyber Security Strategy – designed to ensure that the UK remains resilient in the digital world.

The Department for Science, Innovation, and Technology – known as DSIT – has a key role to play in delivering the strategy and it has implemented a range of initiatives to ensure that digital services and consumer technologies achieve high standards of cyber security.

DSIT has commissioned Pye Tait Consulting, an independent research agency, to conduct work to help it understand current security and privacy practices utilised by app developers - especially the impact and awareness of recent voluntary government initiatives.

Would you be the best person in your business to speak to on this?

- Yes [proceed]
- No [probe to speak to most appropriate person]

Our call today should last around 15-20 minutes. Your feedback will directly help to inform any further support that DSIT might offer to app developers in the future.

Reassurances

The research is being conducted by Pye Tait Consulting on behalf of DSIT. All findings will be treated confidentially and reported anonymously by Pye Tait Consulting under the Data Protection Act 2018, the General Data Protection Regulation (GDPR), and the Market Research Society (MRS) Code of Conduct. A copy of Pye Tait Consulting's Participant Privacy Notice, or of DSIT's privacy notice, is available on request.

If you have any queries about the survey, please contact Tom Wilson, Project Manager at Pye Tait Consulting, via [redacted][at]pyetait.com (telephone 01423 509433). If you have any queries about the project as a whole, please contact the App Developer Survey team at DSIT via [redacted][at]dsit.gov.uk.

Section 0: Screener

- Does your business work in the UK as an app developer, or – if your app developer business is based abroad – are your apps used by UK-based consumers?

By an app developer, we mean any company that either leads in developing the app or contributes to developing segments or elements.

Yes	
No	

If No – thank and close (screen out).

Section 1: About you and your business

1. What is your name, job role, and organisation name? These will be kept in confidence by Pye Tait and not shared with DSIT.

Name	
Job role	
Organisation	

2. How many people does your organisation currently employ (full-time equivalent)?

Please include any staff who may work on your apps in other countries who are employed by your organisation.

Total directly employed	
Total sub-contracted (e.g. freelancers)	
Total staff (auto-filled)	

3. Where is your organisation based or headquartered? **(select one only)**

East of England	
East Midlands	
London	
North East	
North West	
South East	
South West	
West Midlands	
Yorkshire and the Humber	
Northern Ireland	
Scotland	
Wales	
Other	

4. **(only ask if previous q=other)** Please specify in which country your organisation is based if not the UK **(select one only)**.

France	
Germany	
Ireland	
Japan	
Netherlands	
South Korea	
USA	
Other (specify)	

(only ask if previous q=other) If other please specify which country.

5. For which platforms does your organisation develop apps? (Select all that apply)

Mobile	
Laptops/desktops	
Smart TVs	
Games consoles	
Voice assistant platforms	
Wearable devices	
Other (specify)	

If other, please specify.

If only select other, thank and close (screen out).

6. What app stores do you develop apps for? (select all that apply)

Amazon App Store	
Apple App Store	
Google Play	
LG Content Store	
Microsoft Store	
Nintendo eShop	
PlayStation Store	
Samsung Galaxy Store	
Samsung TV Smart Hub	
Other (specify)	

If other, please specify.

7. And in which sector(s) do you develop apps? (Select all that apply)

Accommodation and food	
Administration and support	
Agriculture	
Arts, entertainment, and recreation	
Construction	
Education	
Financial services	
Health and social care	
IT and communications	
Manufacturing	
Professional and technical	
Public sector and defence	
Real estate activities	
Retail and wholesale	
Transport	
Utilities	
Other services	

Current security and privacy practices

DSIT is seeking to understand the security and privacy practices and procedures used by app developers that trade within the UK.

8. To what extent do you do any of the following for the apps you develop? (Select one option per row. If not applicable, please leave blank)

	We do this for all apps we develop	We do this for most (over half) but not all apps we develop	We do this for fewer than half of apps we develop	We do not do this for any of the apps we develop	Unsure
Use industry standard encryption					
Ensure primary function of an app continues if a user chooses to disable optional functionality (e.g. location data)					
Ensure an app only requires the enabled functions and permissions necessary to operate if the user is not presented with any optional functionalities ⁶					
Ensure you do not request permissions which are not required by the app					
Share the permissions requested by the app with the app store operator (to allow this to be cross-checked)					
Take steps to ensure your app adhere to minimum security and data protection requirements ⁷					
Ensure there is a simple uninstall process					
Have a process to readily update and monitor your software dependencies ⁸ in all published versions of an app					
Provide users with a mechanism to delete locally held data, and request deletion of personal data gathered by an app					
Have a vulnerability disclosure process, (such as contact details or a contact form) which you maintain					
Provide updates to fix security vulnerabilities					
Update apps when a third-party library or software development kit (SDK) that they are using receives a security or privacy update					

⁶ Interviewer note: If further clarification required, e.g. not defaulting to requesting more permissions than needed in order to function

⁷ Interviewer note: If further clarification required, by this we mean ensuring the app safeguards users' personal data and abides to data protection law including GDPR

⁸ Interviewer note: Software dependency – third-party coded software used within an app

9. (mask: only show rows in this q where response=over half, under half, or none in previous q) You say you do not fully align your activities with at least one of the statements presented previously. Do you have an organisational plan in place to ensure the apps you develop meet the following elements over the next 12 months? (select one option per row)

	Yes	No – but we have a plan to do so over a longer timeframe	No plan in place	Unsure
Use industry standard encryption				
Ensure primary function of an app continues if a user chooses to disable optional functionality (e.g. location data)				
Ensure an app only requires the enabled functions and permissions necessary to operate if the user is not presented with any optional functionalities ⁹				
Ensure you do not request permissions which are not required by the app				
Share the permissions requested by the app with the app store operator (to allow this to be cross-checked)				
Take steps to ensure your app adhere to minimum security and data protection requirements ¹⁰				
Ensure there is a simple uninstall process				
Have a process to readily update and monitor your software dependencies ¹¹ in all published versions of an app				
Provide users with a mechanism to delete locally held data, and request deletion of personal data gathered by an app				
Have a vulnerability disclosure process, (such as contact details or a contact form) which you maintain				
Provide updates to fix security vulnerabilities				
Update apps when a third-party library or software development kit (SDK) that they are using receives a security or privacy update				

⁹ Interviewer note: If further clarification required, e.g. not defaulting to requesting more permissions than needed in order to function

¹⁰ Interviewer note: If further clarification required, by this we mean ensuring the app safeguards users' personal data and abides to data protection law including GDPR

¹¹ Interviewer note: Software dependency – third-party coded software used within an app

10. (only ask if no plan in place for any row) Please could you explain why you have no plan in place? (select all that apply) (do not read out options)

Not an organisational priority	
Feel existing procedures are sufficient	
Too time-consuming	
Too costly	
Too technically demanding	
Not applicable to all our apps (specify)	
Other (specify)	

If not applicable to all apps – please explain why you feel this is not applicable to all your apps.

If other please explain other reasons why you have no plan in place.

11. To what extent do you provide the following information about the behaviour of apps you develop? (Select one option per row. If not applicable, please leave blank)

	We do this for all apps we develop	We do this for most (over half) but not all apps we develop	We do this for fewer than half of apps we develop	We do not do this for any of the apps we develop	Unsure
Where a user's data is stored, shared and processed within a privacy policy					
When the app was last updated					
Any other relevant security information (specify)					

If other selected for all/most/some apps: please specify what other information you provide.

12. If you become aware of a security incident in an app you've developed which involves a personal data breach, to what extent do you do any of the following? (Select one option per row. If not applicable, please leave blank)

	We do this for all apps we develop	We do this for most (over half) but not all apps we develop	We do this for fewer than half of apps we develop	We do not do this for any of the apps we develop	Unsure
Inform other relevant stakeholders including app store operators, and library/SDK developers					
Assess the impact of the incident and follow appropriate steps set out under data protection law					
Inform affected users and signpost instructions for users to protect themselves					

13. (mask: only show rows in this q where response=over half, under half, or none in previous two qs) You say you do not fully align your activities with at least one of the statements presented previously. Do you have an organisational plan in place over the next 12 months to ensure the apps you develop...? (select one option per row)

	Yes	No – but we have a plan to do so over a longer timeframe	No plan in place	Unsure
Specify where a user's data is stored, shared and processed within a privacy policy				
Specify when the app was last updated				
Provide any other relevant security information				

and in the event of any security breach involving personal data, do you have a plan in place over the next 12 months for the apps you develop to ensure you...?

	Yes	No – but we have a plan to do so over a longer timeframe	No plan in place	Unsure
Inform other relevant stakeholders including app store operators, and library/SDK developers				
Assess the impact of the incident and follow appropriate steps set out under data protection law				
Inform affected users and signpost instructions for users to protect themselves				

14. (only ask if no plan in place) Please could you explain why not? (select all that apply) (do not read out options)

Not an organisational priority	
Feel existing procedures are sufficient	
Too time-consuming	
Too costly	
Too technically demanding	
Not applicable to all our apps (specify)	
Other (specify)	

If not applicable to all apps – please explain why you feel this is not applicable to all your apps.

If other please explain other reasons why you have no plan in place.

Keeping up to date on security and privacy matters

15. Specifically in relation to matters focusing on app development security and privacy, which sources of information have you accessed or used in the past 12 months?
(select all that apply) (present options in random order, keeping bottom two options fixed in place)

The App Association (ACT)	
The Developers Alliance	
The Mobile Growth Association	
Business Application Software Developers Association (BASDA)	
National Cyber Security Centre (NCSC)	
Information Commissioners Office (ICO)	
App store operators	
Industry newsletters	
Any other Government departments or organisations	
Other source(s) (specify)	

If other – please specify which other source/s you have accessed to gather information on matters relating to app development security and privacy.

16. (don't ask each option if do not hear from that source in previous q) How useful would you rate the information provided by each of these sources, in relation to app development security and privacy, on a scale from 1 (not at all useful) to 10 (extremely useful)?

The App Association (ACT)	
The Developers Alliance	
The Mobile Growth Association	
Business Application Software Developers Association (BASDA)	
National Cyber Security Centre (NCSC)	
Information Commissioners Office (ICO)	
Any other Government departments or organisations	
App store operators	
Industry newsletters	
Other source(s)	

17. (only ask if score 6 or below) You gave a score of 6 or below. Please can you briefly explain why the information provided is not as useful as it might be and specify which source this is in relation to.

Maintaining minimum security and privacy requirements

18. Very approximately, what proportion of the apps you develop, are initially rejected by the app store operator (on first submission) on the grounds of security or privacy concerns? Please enter a whole number between 0% and 100%.

19. (only ask if previous q >0%) In such instances, do app store operators provide you with actionable feedback to be compliant with security and privacy requirements? (select one only)

Yes – in all such instances	
Yes – in most such instances	
Yes – but only occasionally	
No, never	
Unsure	

20. (only ask if earlier q >0%; mask so only show stores for which develop apps) Which app store operators rejected your submissions? (select all that apply)

Amazon App Store	
Apple App Store	
Google Play	
LG Content Store	
Microsoft Store	
Nintendo eShop	
PlayStation Store	
Samsung Galaxy Store	
Samsung TV Smart Hub	
Other (specify)	

If other, please specify.

21. Please could you outline what standards and best practice guidelines (if any) you are currently using in your app development process? (select all that apply) (do not read out options)

Guidance from the National Cyber Security Centre (NCSC)	
Guidance from membership bodies	
Voluntary Code of Practice introduced in December 2022	
App store operator guidelines	
Own internal company processes / guidelines	
We do not follow any specific best practice guidelines (no other option can be ticked)	
Other (specify)	

If other, please specify.

22. Are you aware of the UK Government’s Code of Practice for app store operators and app developers? (mandatory question)

Yes	
No	

23. (only ask if aware of Code) From what source(s) have you heard about the Code?
(select all that apply) (do not read out)

App store operator	
DSIT/DCMS	
National Cyber Security Centre (NCSC)	
Information Commissioners Office (ICO)	
A colleague	
A peer	
Membership body	
Other (specify)	

If other please specify

24. (only ask if previous q = 'App store operator') Did the app store operator notify you of the Code before or after app submission? (select one only)

Before app submission	
After app submission	
Unsure	

25. (only ask if previous q = 'App store operator') To what extent would you agree or disagree that the app store operator provided information related to the Code of Practice in a way that was convenient and easy to access? (select only one) (if unsure, leave blank)

Strongly agree	
Agree	
Disagree	
Strongly disagree	

DSIT launched a voluntary Code of Practice for all app store operators and app developers, in December 2022. It sets out the minimum security and privacy requirements which should be followed by app operators and app developers. The Code comprises eight principles aimed to protect users' privacy and security. Some areas of the Code are mandated through existing legislation, including data protection law.

While you may or may not be aware of the Code of Practice, we are keen to understand what actions you are already taking in this area, and what further support may be required to ensure app developers can adhere to the principles therein.

26. (only ask if aware of Code) To what extent has the Code of Practice influenced the security and privacy processes you currently have in place when developing apps, on a scale from 1 (no influence) to 10 (highly influential)?

Please briefly explain your answer.

27. (only ask if aware of Code) What do you see as the main challenges to implement/align to the Code of Practice (if any at all)? (select all that apply) (do not prompt)

Familiarising ourselves with the Code's requirements (lack of current detailed awareness/understanding)	
Cost to implement any changes	
Time to make any changes	
Lack of guidance/support to make necessary changes	
Will result in apps not aligning to other countries' requirements	
Do not see any challenges (no other option can be selected)	
Other (specify)	

If other, please specify

28. (only ask if aware of Code) Please indicate your level of agreement with the following statements. (if unsure or not applicable leave blank)

The Code of Practice....

	Strongly agree	Agree	Disagree	Strongly disagree
Has helped us establish more robust security and privacy procedures				
Has increased our confidence in our security and privacy procedures				
Was easy to integrate within our existing processes and procedures				
That provides key principles for app security and privacy will be helpful for the app developer industry				

29. (only ask if unaware of Code) To what extent do you agree or disagree that introducing a set of voluntary guidelines relating to app security and privacy will be helpful for the app developer industry? (Select one only) (if unsure leave blank)

Strongly agree	
Agree	
Disagree	
Strongly disagree	

(only show this section to those who are aware of the Code) **Cost of implementation and support required**

In this final section, we'd like to understand the approximate costs associated with implementing the Code of Practice for developers.

Please note that – for the following questions – we wish to gather estimates that are additional, i.e. costs for activities that would not otherwise have been incurred were it not for having to adhere to the Code.

30. Thinking about the time and job roles of the people in your organisation who would be involved in implementing the principles outlined in the Code, what would be the estimated cost (in £GBP) for your organisation for each of the following elements:

Familiarise yourself with the Code of Practice	
Scope, develop, test and implement new/revised processes required to adhere to the Code's requirements	
Legal costs	
Other costs (specify)	

If other – please specify details of what other costs you might incur and an estimate of the cost in £GBP. For example, this might include materials/consumables and any internal administrative costs.

31. Bearing this cost estimate in mind, please can you indicate the extent to which the costs associated with implementing the Code might impact your business, on a scale from 1 (no impact at all) to 10 (very significant impact)?

Please briefly explain your answer.

32. What non-financial support (if any) would help you adhere to the principles contained in the Code of Practice? (select all that apply) (do not read out)

Signposting to the Code by app store operators	
Signposting to the Code's detail by another organisation or source (specify)	
Guidelines on how to adhere to the Code from app store operators	
Guidelines on how to adhere to the Code from DSIT	
Guidelines on how to adhere to the Code from another organisation or source (specify)	
Government awareness campaign of the Code	
Mentoring with 'leading' app developers who can share best practice	
Other (specify)	

If signposting by another org – please specify which type/name of organisation you'd welcome signposting from.

If guidelines on how to adhere from another org – please specify which type/name of organisation you'd welcome guidelines from.

If other – please specify what other support would be helpful.

(only show this section to those who are unaware of the Code) Cost of implementation and support required

In this final section, we'd like to understand the approximate costs associated with implementing a set of voluntary guidelines relating to app security and privacy for developers.

Please note that – for the following questions – we wish to gather estimates that are additional, i.e. costs for activities that would not otherwise be incurred were it not for having to adhere to additional guidelines.

33. Thinking about the time and job roles of the people in your organisation who would be involved in implementing a set of voluntary guidelines, what would be the estimated cost (in £GBP) for your organisation for each of the following elements:

Familiarise yourself with the guidelines	
Scope, develop, test and implement new/revised processes required to adhere to the requirements of the guidelines	
Legal costs	
Other (specify)	

If other – please specify details of what other costs you might incur and an estimate of the cost in £GBP. For example, this might include materials/consumables and any internal administrative costs.

34. Bearing this cost estimate in mind, please can you indicate the extent to which the costs associated with implementing a set of voluntary guidelines relating to app security and privacy might impact your business, on a scale from 1 (no impact at all) to 10 (very significant impact)?

Please briefly explain your answer.

35. What non-financial support (if any) would help you adhere to a set of voluntary guidelines relating to app security and privacy? (select all that apply) (do not read out)

Signposting to the guidelines by app store operators	
Signposting to the guidelines by another organisation or source (specify)	
Guidelines on how to adhere from app store operators	
Guidelines on how to adhere from DSIT	
Guidelines on how to adhere from another organisation or source (specify)	
Government awareness campaign of the guidelines	
Mentoring with 'leading' app developers who can share best practice	
Other (specify)	

If signposting by another org – please specify which type/name of organisation you'd welcome signposting from.

If guidelines on how to adhere from another org – please specify which type/name of organisation you'd welcome guidelines from.

If other – please specify what other support would be helpful.

Final comments

36. Do you have any final comments you would like to add about the Code of Practice or security and privacy practices in app development?

--

We will also be holding follow-up interviews with app developers to explore this topic in more detail, and to gather suggestions on where or how the Code could be improved in terms of its implementation and presence across the sector, and what future support might be required.

Our discussion will take place over telephone or MS Teams at a time that suits you over the next couple of weeks.

37. Is this something that you are willing to participate in?

Yes	
No	

38. (If yes) Thank you, please provide your contact details and a member of the research team will shortly be in touch to arrange this with you.

Email	
Telephone	

Thank and close.

Interview topic guide

App Developers Security and Privacy Practices: the Code of Practice

Introduction

Thank you for taking the time recently to complete our survey, and for expressing interest in a follow-up interview.

To recap, the Department for Science, Innovation & Technology (known as DSIT) has a key role to play in delivering the UK government's national cyber security strategy. It has implemented a range of initiatives to ensure digital services and consumer technologies achieve high standards of cyber security.

One such initiative introduced by DSIT in December 2022 was the voluntary Code of Practice for app store operators and app developers. It sets out the minimum security and privacy requirements which should be followed by app operators and app developers. Some areas of the Code are mandated through existing legislation, including data protection law.

DSIT commissioned Pye Tait Consulting, an independent research agency, to explore the awareness and impact of the Code among app developers, which today's conversation will delve into further. Hopefully you will have had chance to briefly familiarise yourself with the Code ahead of today's conversation using the link we shared in advance.

Our discussion today should last around 45 minutes and your feedback will directly help to inform any further support that DSIT might offer to app developers in the future.

Reassurances

The research is being conducted by Pye Tait Consulting on behalf of DSIT. All findings will be treated confidentially and reported anonymously by Pye Tait Consulting under the Data Protection Act 2018, the General Data Protection Regulation (GDPR), and the Market Research Society (MRS) Code of Conduct. A copy of Pye Tait Consulting's Participant Privacy Notice, or of DSIT's privacy notice, is available on request.

If you have any queries about the research, please contact Tom Wilson, Project Manager at Pye Tait Consulting, via [redacted][at]pyetait.com (telephone 01423 509433). If you have any queries about the project as a whole, please contact the App Security and Privacy team at DSIT via [redacted][at]dsit.gov.uk.

Please note that we will record this call – purely for our own internal use to ensure we have accurate notes. This will be automatically deleted after 60 days.

Interviewer to pre-fill from survey

Interviewer name	
Respondent name	
Job role	
Organisation	
Region/Nation	
Business size	
Aware of Code? (survey Q22) (Y/N)	

Part 1: Guidance used to develop apps

I'd like to start by understanding how your organisation goes about developing apps in general. Firstly...

1. What legislation and/or guidance (if any) does your organisation use to guide the development of your apps for the UK market?

Probe: what sources do you use? Is there a 'standard' procedure or process each app follows in its development? Do you have internal guidelines to follow too?

2. How helpful (or not) is this guidance and/or legislation for your app development? Why do you say that?

Probe: which sources are more/less useful – with reasons.

3. In general, how closely do you engage with app store operators? Do you have a key/named point of contact? And does this vary by app store?

Probe: a general question asking about frequency/level of communication in general (not just related to security and privacy practices).

4. Can you tell me about the level of support or guidance you receive from app store operators (if any) relating to app privacy and security?

Probe: do they receive regular (general) updates? And/or do they get specific feedback about their apps (e.g. if rejected or removed from the store)?

5. How helpful (or not) is it? Do you have chance to discuss apps and/or feedback with app stores?
6. What other guidance (if any) would be helpful for your organisation when developing apps for the UK market?

Probe: from whom, and what content/detail might be useful – with reasons

Part 2: Current security and privacy practices

I'd now like to understand a bit more about your current app security and privacy practices.

7. When developing apps, what are the main security and privacy practices you always implement?

Prompt if needed: using encryption, ensuring primary functionality works if user disables optional functionality, ensuring users have a simple uninstall process, process to readily update software and to fix vulnerabilities

8. What is the driver for these adapting these security and privacy practices? To what extent (if at all) has the Code influenced your business to undertake any of these practices?

Probe: Moral duty, to abide to legislation, whether Code has impacted activities (which practices?)

9. How frequently do you update your apps? What drives this?

Probe: Are updates done on a regular basis (how often), or ad hoc when vulnerabilities are identified, or ad hoc when a third-party provides updates?

10. And if/when a personal data breach were ever to occur in an app you develop, please could you outline briefly what steps you would follow in the aftermath in terms of who you would notify?

Probe: report to app store operator or to third-party software developers? Inform users?

11. And what level of information or guidance (if any) might you provide to app users in such a situation?

Part 3: Implementing the Code of Practice

12. When you responded to the survey, you said that you were (not) aware of the Code. To what extent do you feel further promotion – if any – is required to raise awareness of the Code among app developers?

Probe: from who? What would be the most effective means of communicating this? What could/should this info contain?

13. Hopefully you had chance ahead of our call to look at the Code. How easy or difficult did you find it to digest the information and principles within Code? Could the information be conveyed any differently?

Probe: Is it too detailed/complex/long, or not? Would a shorter version work for developers or not – what format might this be in, what information could it contain?

14. From your review, did you feel there was any gaps in the Code, or anything you were expecting to see that was not included?

15. How easy or difficult do you think it will be to implement the Code? Why do you say that?

Probe: are they doing this already? What barriers do they envisage?

16. What non-financial support (if any) would you require to implement the principles within the Code?

Probe: from who? What support do you need?

17. And to what extent do you envisage that implementing the principles within the Code might place a financial burden on your organisation (if at all)?

Probe: what activities might attract cost, and how much (ballpark figure) in total or per activity?

18. And finally, to what extent do you feel that the Code might influence your organisation's growth in the UK market? Why do you say that?

Probe: will the Code be a burden, or will it provide reassurance to strengthen offering?

Part 4: Final comments

19. Do you have any final comments you would like to add about the Code of Practice or security and privacy practices in app development?

Thank and close.

A report prepared by:

Pye Tait Consulting

Registered in England, Company No: 04001365, VAT No: 755 8312 14

Postal address: Royal House, 110 Station Parade, Harrogate, North Yorkshire, HG1 1EP

Tel: 01423 509 433

Registered office address: 5 Merus Court, Meridian Business Park, Leicester, LE19 1RJ

email (enquiries related to this report): n.charleton@pyetait.com

email (general enquiries): info@pyetait.com

website: www.pyetait.com



Pye Tait Consulting is part of the EMB-Group.

Pye Tait Consulting is a member of:

