Department for Science, Innovation, & Technology

# Survey of App Developers

## Final report

February 2024

# Contents

# Executive summary

Applications, commonly known as apps, have become essential to modern life in the UK. Generally, apps are downloaded from an app operator's store or are pre-installed on many devices. Millions of apps are available to download, and since it is unlikely that many users have an extensive awareness of security issues or an app's trustworthiness or reliability, they are dependent on app stores and developers to provide only legitimate and non-harmful apps.

As part of its ambition to deliver on objectives in the National Cyber Strategy, the Department for Science, Innovation, and Technology's (DSIT/the Department) has implemented a range of initiatives to ensure that digital services and consumer connected technologies follow better standards of cyber security. Following a public consultation, the UK government developed a voluntary Code of Practice ("the Code") for all app store operators and app developers.[1] The Code, published in December 2022, sets out the minimum security and privacy requirements which should be followed by app store operators and app developers to protect UK consumers.

The Code is voluntary and contains eight principles which at present, apply to six categories of devices (detailed in section 1.1.2). Operators and developers have been given until June 2024 to implement the Code. DSIT has commissioned various research, including this survey, undertaken by Pye Tait Consulting from August to November 2023, to monitor the Code's uptake.

## Aims

The overarching aims of this research were to assess app developers' awareness of specific principles in the Code and to test whether they are implementing the baseline requirements within their apps. The research also sought to understand the costs involved with implementing the requirements. An additional intention of this first-of-a-kind study was to understand more clearly the firmographic profile of the app developer population.

More detailed objectives are in section 1.2.

## Methodology

The research comprised three core methodological strands.

- **Mapping exercise** to understand the size and scale of the UK app developer population to inform the sampling approach.
- **Survey of 600 app developers** (539 UK-based and 61 based abroad) via telephone and online in October and November 2023.

[1] DSIT, 2022, Code of Practice for app store operators and app developers – see https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers accessed 15 December 2023

- **In-depth interviews** with 20 UK-based app developers in November 2023 to add further detail and build on survey responses.

## Key findings

### Shape of the sector

The majority (70%) of surveyed app developers are 'micro' in size (fewer than 10 employees). The most common size of business is two directly employed staff, with the mean average of 18 being skewed by a small number of larger companies. This is similar to the 'normal' business population of other sectors, where the vast majority of businesses within a sector are micro or small in size.[2]

### Awareness of the Code

Just under one in six (16%) surveyed app developers are aware of the UK Government's Code of Practice for app store operators and app developers. Awareness increases with company size ranging from 12% among micro firms to 33% among medium (50 to 249 employees) and large (250+ employees) businesses. Awareness is highest among those developing apps for voice assistant platforms (31%) and games consoles (25%), and lowest among those developing apps for laptops/desktops (15%) and mobile devices (14%).

Developers most commonly heard of the Code via app store operators (35%), DSIT/DCMS (23%) or a membership body (22%). Of those that were signposted to the Code by operators, the majority said this was prior to app submission, and that the information was useful.

### Current security and privacy practices

There are varying degrees of alignment to each of the Code's principles – for several of the Code's principles over 80% say their security and privacy practices align for all apps they develop, while for other principles alignment stands between 50% and 60%. This variation is due to a large extent on app developers' circumstances and whether all principles are necessarily applicable (for instance if their apps do not process or store personal data, or are bespoke and not available via app stores).

However, compared to those aware of the Code, a significantly lower proportion of those unaware of the Code have organisational plans in place to implement certain practices that align to the Code's principles.

Over four in five (82%) share information on when the app was last updated and 74% signpost to where users' data is stored, for all apps they develop. Other information is also provided to users in some situations and this can include additional security information, extra security protocols and encryption. The extent of information and detail that would be provided to users and other parties in the event of a security incident or data breach varies between app developers.

### Influence and impact of the Code

Interviewed app developers discussed how alignment to the Code has helped strengthen opportunities for commercial success by demonstrating adherence to government guidelines

[2] ONS, 2023, Business Population Estimates

to potential clients. However, some surveyed app developers felt the Code had had limited impact with 12 saying they place greater value on app store operators' guidance due to their role as gatekeepers to an app's publication.

Of app developers unaware of the Code, just under three quarters (74%) agree or strongly agree that introducing a set of voluntary guidelines relating to app security and privacy will be helpful for the app developer industry.

### Support required to adhere to the Code's principles

Among both those aware and unaware of the Code, a government campaign to raise awareness of the Code is commonly suggested (31% and 66%, respectively). Confirming this, the majority (17 of 20) of interviewees feel the Code must be marketed and promoted further to have a significant impact on the industry. Six went on to discuss how the Code represents a chance to set a benchmark for the industry to follow and to ensure a minimum standard of privacy and security, particularly because it is endorsed by government.

Eight interviewees explicitly noted that the Code is straightforward and clear. However, three suggested the Code could be more interactive or visual or disseminated through different mediums to increase engagement.

### Cost of implementation

Just under three in ten (29%) envisage no barriers to implementing the Code, while 30% believe time to implement changes will be a challenge. Estimated costs and their associated impact are seen as relatively low – just under half foresee no financial implication. The median rating of the impact of such costs on the business was five out of 10 for those aware of the Code, and three for those unaware, with 15 of 84 (16%) developers who provided further comment saying their security and privacy practices already align to the Code's principles to explain why they provided a rating of between one and three. A minority anticipate greater impacts where more substantial changes to existing processes may need enacting (see section 2.4).

### Keeping up to date on security and privacy practices

The most commonly accessed or used source of information over the last 12 months is that from app store operators (used by 43% of all surveyed app developers) and industry newsletters (25%). The usefulness of information from various sources is generally rated highly (each source received an average rating of 7.7 out of 10 or higher).

Most (60%) have their own internal processes to follow when developing apps, while guidelines from operators are also followed by over two in five (44%). GDPR is also a key source guiding app development, especially when dealing with personal data.

### Engagement with app store operators

Developers say this tends to be on an ad hoc basis, and only when deemed necessary as circumstances dictate. For instance, operators will engage with developers when an app is rejected or accepted.

The average (mean) proportion of apps rejected by operators on the basis of security and privacy is 5%. It was suggested that operators' contact with developers is more regular or personalised for developers whose apps have a larger number of users, with a few noting it was difficult to get in contact with operators.

# 1. Introduction

## 1.1 Background

### 1.1.1 Apps as part of everyday life

Applications, commonly known as apps, have become essential to modern life in the UK. Smartphone usage has increased 200% from 2009 to 2022,[3] and 94% of the UK's online adult population use apps on smartphones or tablets.[4]

Apps have been commonly used for leisure, work, and everyday utility, and there has been increasing deployment of apps across government.

Generally, apps are downloaded from an app operator's store or are pre-installed on many devices. Millions of apps are available to download, and since it is unlikely that many users have an extensive awareness of security issues or an app's trustworthiness or reliability, they are dependent on app stores and developers to provide only legitimate and non-harmful apps.

Security and privacy issues are not limited to mobile and desktop devices. For example, through their link with smartphones, health information collected by wearable devices can be accessed. Across gaming consoles, 87% of surveyed Xbox users said they had been targeted by hacking and scams, requiring gaming companies to recognise the critical role they play in protecting their applications and users.[5] Cameras and microphones on smart televisions are susceptible to malware installation, while hackers can take control of voice assistant platforms.[6]

### 1.1.2 Developing a Code of Practice

In 2022, the government published its National Cyber Strategy which details plans to ensure that the UK remains confident, capable, and resilient in this fast-moving digital world, and that the UK continues to adapt, innovate, and invest to protect and promote its interests in cyberspace.[7]

The Department for Science, Innovation, and Technology (DSIT/the Department) leads on the technology advantage pillar and UK cyber ecosystem pillar, and co-leads on the cyber resilience pillar of the National Cyber Strategy. As part of the Department's work on this, it

[3] Statista.com (2023) https://www.statista.com/statistics/300452/mobile-phone-use-to-go-online-uk/ accessed 12 December 2023
[4] Ofcom, 2021, Online nation
[5] J. Casey, 2023, Infosecurity magazine https://www.infosecurity-magazine.com/opinions/gaming-console-secure-priority/ accessed 15 December 2023
[6] For example, security research detailed a technique to install malware on an Amazon Echo device that would silently stream audio from the hacked device to a specified server. See Forbes.com (2017) https://www.forbes.com/sites/jaymcgregor/2017/09/07/listening-in-on-a-hacked-amazon-echo-is-terrifying/ accessed 9 January 2024
[7] HM Government, 2022, National Cyber Strategy

has implemented a range of initiatives to ensure that digital services and consumer connected technologies follow better standards of cyber security.

Following a public consultation,[8] the UK government developed a voluntary Code of Practice ("the Code") for all app store operators and app developers.[9] The Code, published in December 2022, sets out the minimum security and privacy requirements which should be followed by app store operators and app developers. The government believes this Code will help protect UK users from malicious and poorly developed apps. The Code consists of eight principles which are not ranked in a priority order as they are all equally important in helping to protect users' privacy and security. Some areas of the Code are mandated through existing legislation, including data protection law. The eight principles are as follows, which vary in whether they primarily apply to app store operators (O), app developers (D), and/or platform developers (P).[10]

1. Ensure only apps that meet the Code's security and privacy baseline requirements are allowed on the app store (O).
2. Ensure apps adhere to baseline security and privacy requirements (D,P).
3. Implement a vulnerability disclosure process (D,O).
4. Keep apps updated to protect users (D,O,P).
5. Provide important security and privacy information to users in an accessible way (D,O).
6. Provide security and privacy guidance to Developers (O).
7. Provide clear feedback to developers (O).
8. Ensure appropriate steps are taken when a personal data breach arises (D,O).

The Code of Practice covers apps provided across various devices.

- Mobile
- Laptops/desktops
- Smart TVs
- Games consoles
- Voice assistant platforms
- Wearable devices

As the Code is voluntary, it is necessary to monitor its uptake and to understand how this work can be progressed in order to better protect users. To that end, in Autumn 2023, DSIT commissioned Pye Tait Consulting to investigate the awareness and impact of the Code among app developers.

[8] DCMS, 2022, App security and privacy interventions – see: https://www.gov.uk/government/consultations/app-security-and-privacy-interventions accessed 15 December 2023
[9] DSIT, 2022, Code of Practice for app store operators and app developers – see https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers accessed 15 December 2023
[10] The Code defines platform developers as: Persons or organisations responsible for producing the operating system, default functionality and the interface that enables third parties to implement additional functionality, such as through apps.

## 1.2 Aims and objectives

The overarching aim was to assess app developers' awareness of specific principles in the Code and to test whether they are implementing the baseline requirements within their apps. The research was also used to understand the costs involved with implementing the requirements, and how costs and compliance levels differ across the different groups of developers. Specific objectives were as follows.

1. Assess app developers' awareness of the Code of Practice (see section 2.1), their views on barriers to uptake of the Code (section 2.5), and what has driven some developers to take up the Code (section 2.5).

2. Understand whether security and privacy practices that app developers currently have in place have been influenced by the Code of Practice (Principles 2, 3, 4) (sections 3.1.1 and 3.2).

3. Understand how app developers provide security and privacy information to users in an accessible way (Principle 5) (section 3.2.3).

4. Understand what steps or processes are in place by app developers if they become aware of a security incident or a personal data breach (Principle 8) (section 3.2.3).

5. Understand whether app store operators are signposting the Code of Practice (and other relevant guidance) to developers prior to an app's submission (Principle 6) (section 2.1.2).

6. Understand the prevalence of rejected apps under the Code of Practice and whether app developers have received actionable feedback from app store operators to make the app compliant with the Code of Practice (Principle 7) (section 4.2).

7. Understand where/if app developers get support (i.e. members of bodies etc.) (sections 2.1.2 and 4.1).

8. Understand the costs involved with implementing the requirements of the Code and whether, if fully complying with the Code of Practice, these would cause any business to drop out of the market (section 2.4).

Further, while the primary research aim was to understand awareness and impact of the Code of Practice introduced in December 2022, an additional intention was to understand more clearly the firmographic profile of the app developer population (i.e. characteristics of the population such as company size, regional spread, etc.).

## 1.3 Methodology

The research comprised three core methodological strands.

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

### 1.3.1 Mapping exercise

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 primary fieldwork. This study is the first of its kind among UK app developers, and this mapping was intended as a useful benchmark to help understand the size and scale of the app developer population.

A range of secondary sources were reviewed including official statistics such as ONS published data (business population estimates; business counts; business demography statistics; business survey and employment register). A variety of other secondary sources including freely available reports and statistical releases were also reviewed, including the National Cyber Security Centre's (NCSC's) threat report on application stores,[11] and the ACT App Association's report on the app economy in Europe.[12]

The mapping exercise targeted industry reports and databases for the most part – often, this proved to be a fruitless endeavour, as these were either not accessible or did not contain relevant information.

Desk research identified that there is little available information on the size and scale of the population of app developers. The information that was available provided a ballpark estimate for the overall size of the app developer population, but more granular information about the size and scale of the population was not available. 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 was very little information available on the profile of app developers operating in the UK, e.g. the population's breakdown by size.

While app developers do not clearly fall into one SIC code, two were identified as being the most likely for which app developer businesses would fall under.[13] Due to the limitations of other data sources consulted as part of the desk review, and the credibility that can be placed on official statistical data, these SIC codes were therefore 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), and
- 6202 computer consultancy.

As part of the mapping exercise, the most relevant SIC code is 6201, so greater weighting was placed on 6201 over 6202, with a 70:30 split in calculating population estimates and sampling targets.

One key source identified in the desk review suggested there are 13,340 app developers in the UK[14] (with other sources providing estimates of a similar size). Splitting this 70:30 gave 9,340 app developers in 6201 and 4,000 in 6202.

[11] National Cyber Security Centre, 2022, Threat report on application stores
[12] ACT App Association, 2022, The App Economy in Europe
[13] Note that businesses self-select which SIC they fall under when registering their company.
[14] IBISWorld (2023) App Development in the UK - Market Research Report

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.

Further details of the mapping exercise and resulting sampling strategy are available in the accompanying technical report.

### 1.3.2 Survey of app developers

A survey questionnaire was designed jointly between Pye Tait Consulting and the Department. The questionnaire explores app developers' current security and privacy practices (aligning questions to the principles within the Code, but not mentioning the Code at this stage), before seeking awareness of the Code (prompted) and the nature and extent of its impact.

Once finalised, the survey was hosted in SNAP XMP online and initial piloting was undertaken with 16 app developers between 2 and 4 October 2023.

Following feedback, the questionnaire was refined and finalised. The survey was live from 13 October to 30 November 2023. The research was promoted on DSIT's webpages and through industry bodies (including The ACT App Association, The Developers Alliance, and Business of Apps), with both online and telephone responses received.

Including the pilot, completions were achieved with a total of 600 app developers, of which 61 were based or headquartered overseas.

Further details of the piloting and a copy of the survey questionnaire are available in the accompanying technical report.

### 1.3.3 In-depth interviews with app developers

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

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. In advance of the conversation, interviewees were sent a copy of the Code to familiarise themselves with this.

### 1.3.4 Notes to the reader

We refer to businesses that contributed to the research through the survey as 'surveyed app developers' or 'respondents'. We refer to those who contributed via in-depth interviews as 'interviewed app developers' or 'participants'.

Note that not all respondents answered all questions.

Some charts and tables may not add to 100% due to rounding.

Any numbers and percentages quoted relate to the particular survey question being discussed, not to the overall total number of research respondents.

Statistical testing was undertaken to identify differences by respondent sub-group (by size, region, platform for which apps are developed, and whether aware of the Code or not). Where such differences exist, these are drawn out in the report and the word 'significant' is used, herein, only to identify statistically significant differences at the 95% confidence level.

## 1.4 Survey respondent and interview participant profiles

### 1.4.1 Survey respondents

The majority of surveyed app developers (70%) are micro firms, directly employing fewer than 10 staff. Around one quarter (27%) are small with between 10 and 49 staff, with a minority being medium (3%) or large (1%).

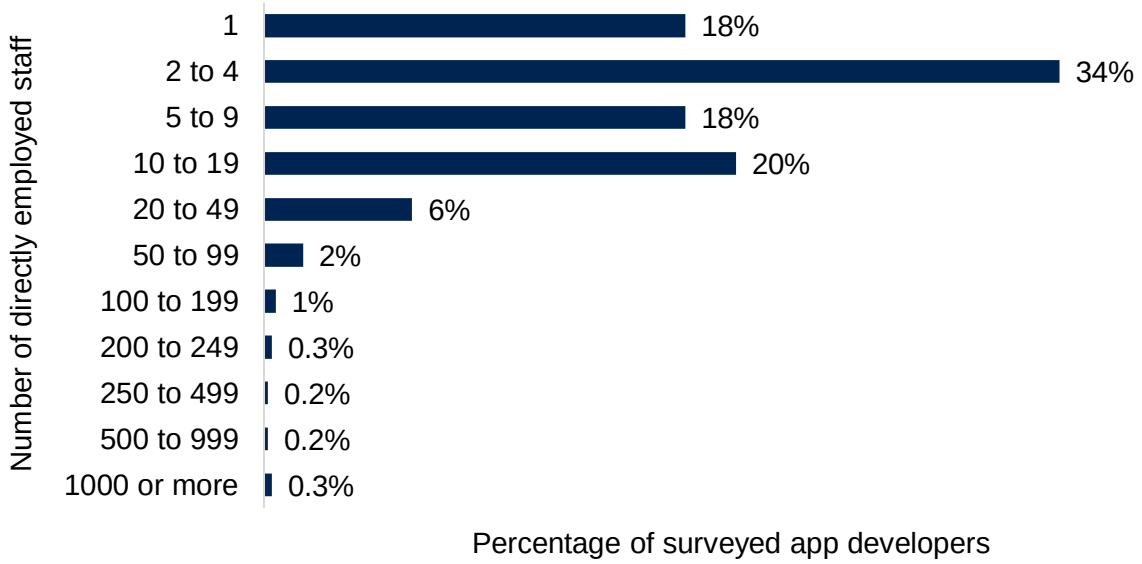
**Table 1 Surveyed app developers' profile by company size (based on employees)**

| Size | Number | Proportion |
|---|---|---|
| Micro (1 to 9) | 420 | 70% |
| Small (10 to 49) | 159 | 27% |
| Medium (50 to 249) | 15 | 3% |
| Large (250+) | 6 | 1% |
| **Total** | **600** | **100%** |

Source: Pye Tait Consulting 2023.

The average (mean) number of directly employed staff is 18, while the most common (modal) size is two, and the median is four. The majority of app developers are micro in size, with the mean average being skewed by a small number of larger companies.

**Figure 1 Distribution of respondents by number of directly employed staff**



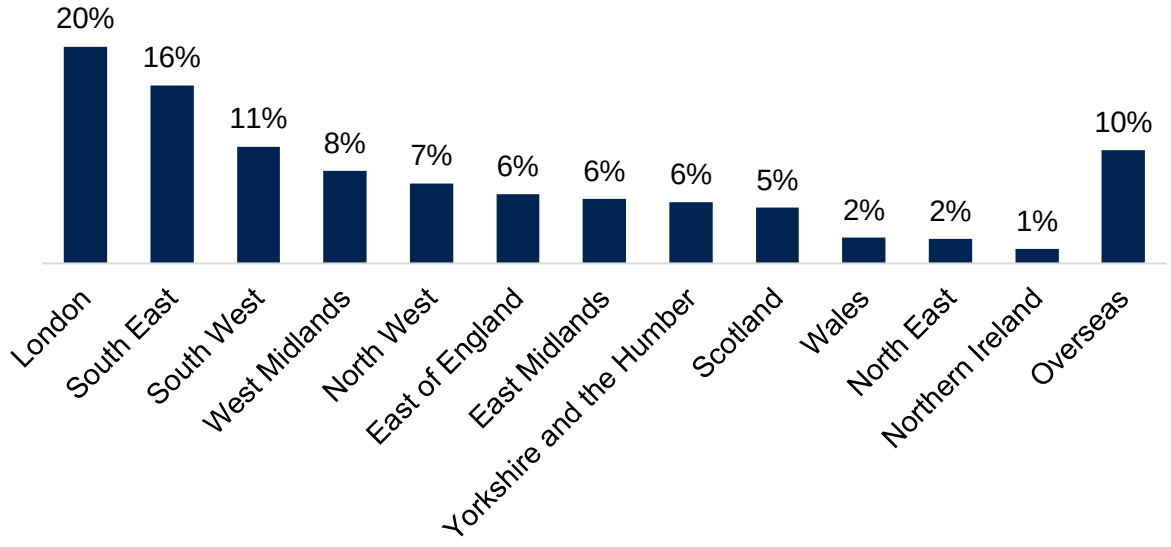

Base: 600 respondents. Source: Pye Tait Consulting 2023.

Around one in seven surveyed app developers (14%) employ sub-contractors – the average (mean) number employed is 11, and the median number is four. This is indicative of a small number of businesses employing a large number of sub-contractors acting to skew the mean average.

In terms of total staff (directly employed plus sub-contractors), the average size is 19 employees, and the median size is five.

Surveyed app developers are based or headquartered across the UK, with most responses from those based in London (20%) and the South East (16%) and fewest from the devolved nations and the North East. One in ten respondents are based overseas reflecting the global nature of the app development sector.

**Figure 2 Regional profile of survey respondents**




Base: 600 respondents. Source: Pye Tait Consulting 2023.

Besides responses from 539 app developers based in the UK, 61 overseas responses were received, with most commonly gathered from app developers based in Germany (3%), USA (1%), and France (0.7%).

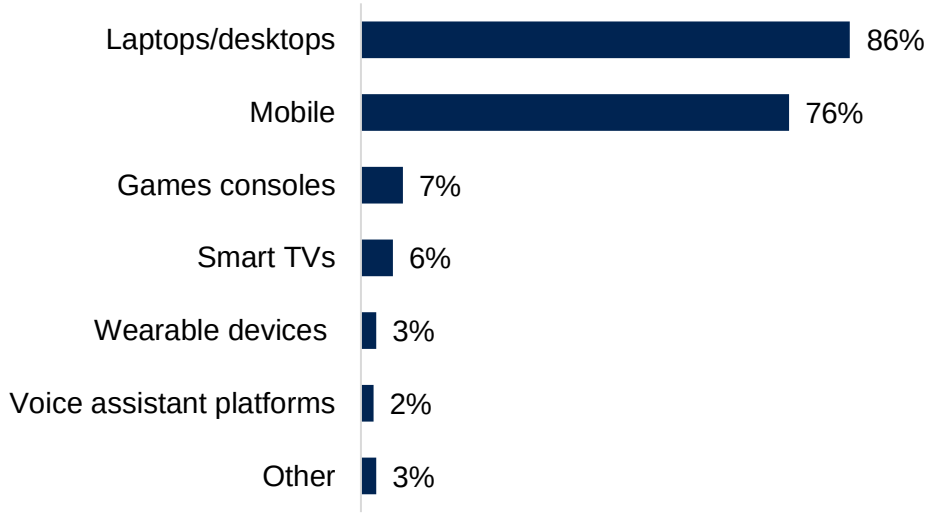
**Table 2 Countries of surveyed app developers based overseas**

| Nation | Count | Nation | Count |
|---|---|---|---|
| Germany | 18 | Romania | 2 |
| USA | 8 | Australia | 1 |
| France | 4 | Bangladesh | 1 |
| Malta | 3 | Belgium | 1 |
| Norway | 3 | Estonia | 1 |
| Poland | 3 | Hungary | 1 |
| Sweden | 3 | Latvia | 1 |
| Austria | 2 | Japan | 1 |
| Italy | 2 | Singapore | 1 |
| Portugal | 2 | Spain | 1 |

Base: 61 overseas respondents. Source: Pye Tait Consulting 2023.

The majority (86%) of surveyed app developers said they develop apps for laptops/desktops, while just over three quarters (76%) do so for mobile devices.

**Figure 3 Platforms for which apps are developed (by app developer)**

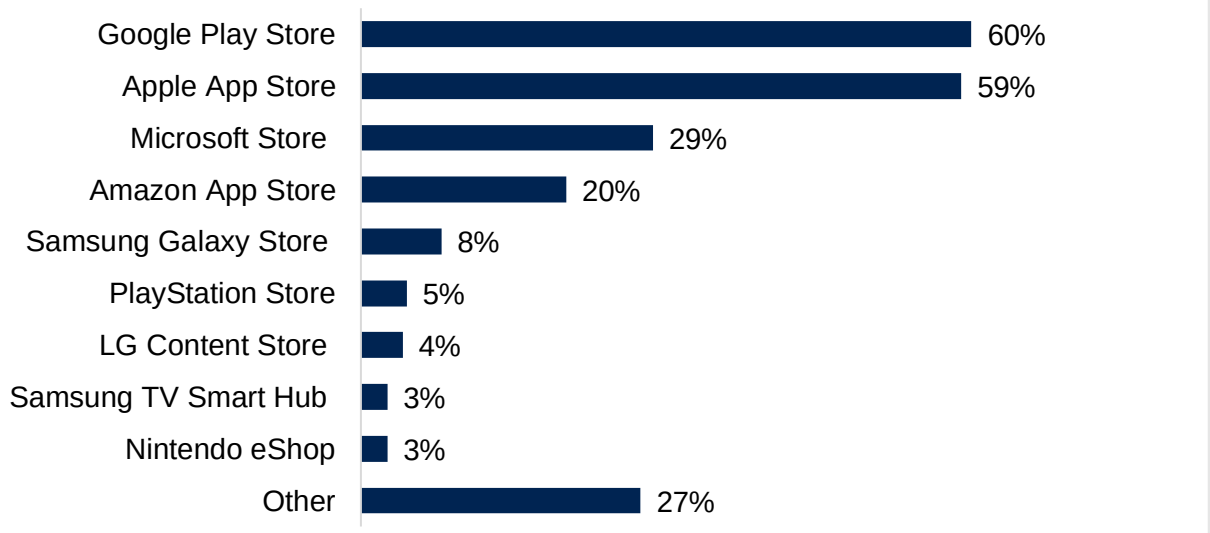



Base: 594 respondents (multiple responses permitted). Source: Pye Tait Consulting 2023.

'Other' platforms mentioned by 16 respondents mostly comprise web based platforms, with a couple noting server/CPU (Central Processing Unit) platforms.

Surveyed app developers most commonly develop apps for Google Play Store (60%) or Apple App Store (59%), with just under three in ten (29%) doing so for the Microsoft store.

**Figure 4 App stores for which apps are developed**

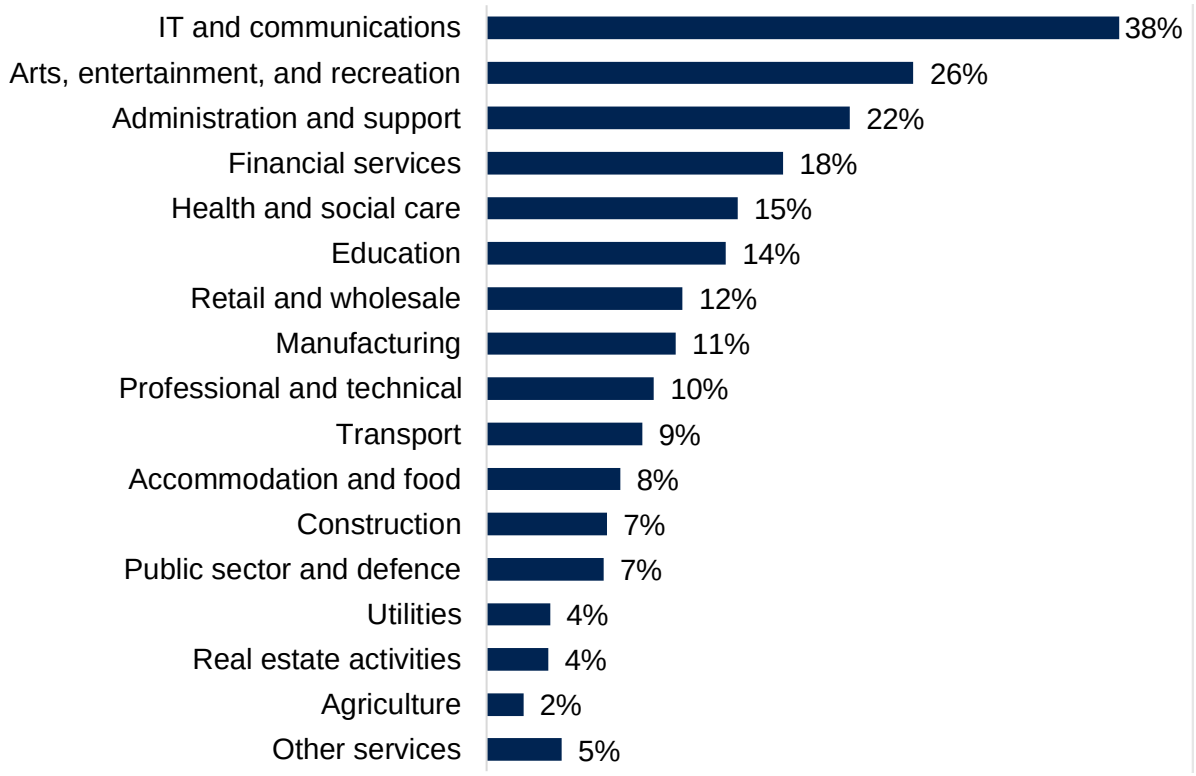



Base:493 respondents (multiple responses permitted). Source: Pye Tait Consulting 2023.

Of the 135 respondents who specify 'other' users, the majority (74, 55%) say they have created apps which are bespoke for specific clients. Several (26, 19%) also say their apps are embedded within web-based designs.

Around two in five (38%) develop apps for use in the IT and communications sector, just over a quarter (26%) for the arts, entertainment and recreation sector, and around one in five (22%) for the administration and support sector.

**Figure 5 Sector for which apps are developed**




Base: 600 respondents (multiple responses permitted). Source: Pye Tait Consulting 2023.

### 1.4.2 In-depth interview participants

The profile of interview participants broadly mirrored that of the survey respondent profile.

The profile of the 20 in-depth interview participants is as follows.

- By size
  - Nine are micro.
  - Eight are small.
  - Two are medium.
  - One is large.

- By region
  - Four are based in the South East.
  - Three are in London.
  - Two each are in the East Midlands, North West, Scotland, South West, and West Midlands.
  - One each is in the East of England, Wales, and Yorkshire and the Humber.

- Five were aware of the Code of Practice prior to participating in the research.

# 2. Code of Practice

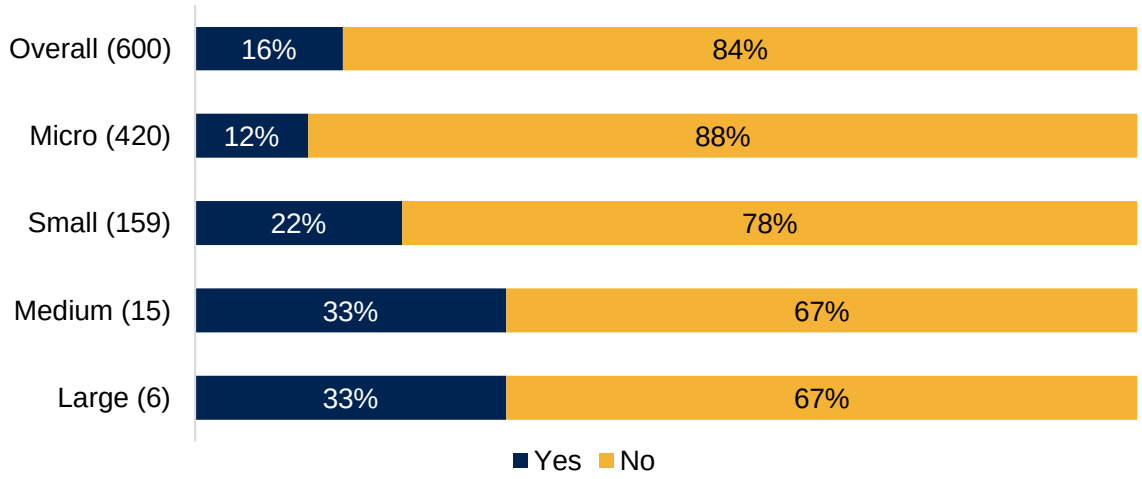
This chapter reveals app developers' level of awareness of the Code, and their current engagement with, and understanding of, the Code. It outlines the influence and impact of the Code to date, and what non-financial support might be valued to help developers adhere to the Code's principles. An estimate of the cost of implementation to align to the Code, and the impact for businesses, is also explored.

## 2.1 Awareness of the Code

Just under one in six (16%) surveyed app developers are aware of the UK Government's Code of Practice for app store operators and app developers.

Awareness increases with company size. One in three (33%) medium and large surveyed app developers are aware of the Code compared to one in eight (12%) micro companies – a significant difference between micro and medium firms.

**Figure 6 Awareness of Code of Practice by company size**




Source: Pye Tait Consulting 2023.

There is some significant regional variation in awareness of the Code – being highest in Northern Ireland (25%) (NB: small sample size) and the North East (23%) and lowest in the North West (5%) and Wales and the South East (both 7%). Surveyed app developers in London and the North East are significantly more likely to be aware of the Code than those in the North West.

There is also some variation by platform. App developers who develop apps for voice assistant platforms have greatest levels of awareness (31%). Meanwhile, those who develop apps for games consoles are significantly more likely to be aware of the Code than those who develop mobile apps.

**Table 3 Awareness of Code of Practice by region, and by platform**

| Region (base) | % aware | | Platform (base) | % aware |
|---|---|---|---|---|
| Northern Ireland (8) | 25% | | Voice assistant platforms (13) | 31% |
| North East (13) | 23% | | Games consoles (44) | 25% |
| London (117) | 18% | | Wearable devices (16) | 19% |
| South West (63) | 16% | | Smart TVs (33) | 18% |
| Yorkshire and the Humber (33) | 12% | | Laptops/desktops (513) | 15% |
| East of England (37) | 11% | | Mobile (449) | 14% |
| East Midlands (35) | 11% | | | |
| West Midlands (50) | 10% | | | |
| Scotland (30) | 10% | | | |
| South East (96) | 7% | | | |
| Wales (14) | 7% | | | |
| North West (43) | 5% | | | |

Note: App developers may develop apps for more than one platform. Source: Pye Tait Consulting 2023.

### 2.1.1 Appetite for introducing a set of voluntary guidelines relating to app security and privacy

Of app developers who were unaware of the Code, just under three quarters (74%) agree or strongly agree that introducing a set of voluntary guidelines relating to app security and privacy will be helpful for the app developer industry.

**Figure 7 Whether voluntary guidelines will be helpful for app developers – those unaware of Code**


Base: 488 respondents. Source: Pye Tait Consulting 2023.

Agreement levels are particularly high among surveyed app developers based in the north of England: Yorkshire and the Humber (96%), North West (85%) and North East (80%), as well as the South East (81%), and lowest in Northern Ireland (67%).

**Table 4 Whether voluntary guidelines will be helpful – for those unaware of Code – by region**

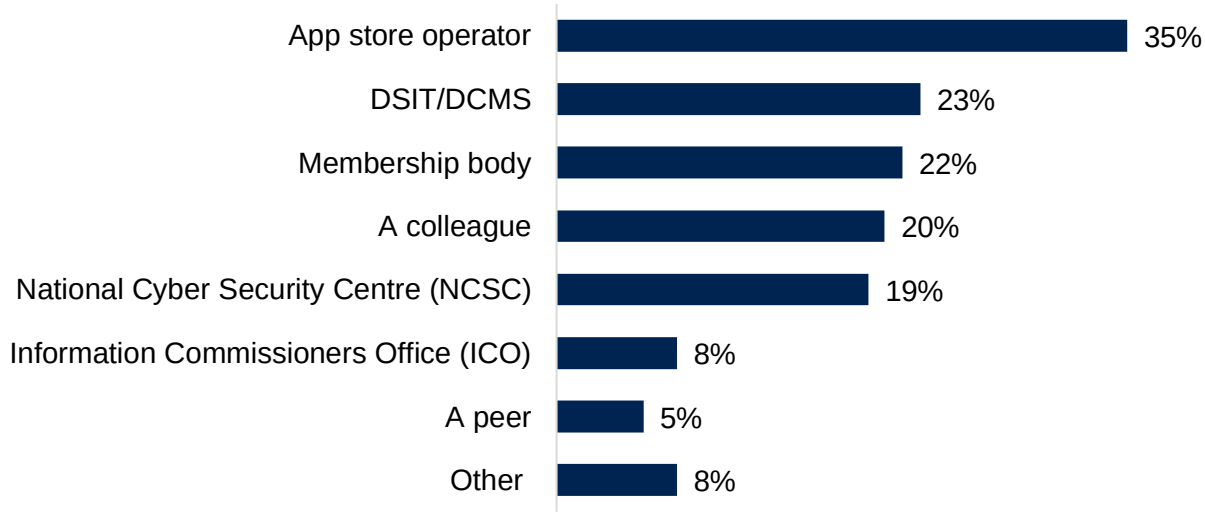
| Region/nation | Strongly agree or agree |
|---|---|
| Yorkshire and the Humber | 96% |
| North West | 85% |
| South East | 81% |
| North East | 80% |
| Scotland | 77% |
| London | 76% |
| West Midlands | 76% |
| Wales | 75% |
| East of England | 71% |
| East Midlands | 71% |
| South West | 70% |
| Northern Ireland | 67% |

Base: 488 respondents. Source: Pye Tait Consulting 2023.

### 2.1.2 How app developers heard of the Code

The 16% of surveyed app developers who were aware of the Code were asked from what source(s) they heard about it. Around one third of these (35%) had heard from an app store operator, around one quarter (23%) from DSIT/DCMS, and around one fifth (22%) from a membership body. One in five (20%) had heard via a colleague, and just under one fifth (19%) from NCSC.

**Figure 8 How app developers aware of the Code heard about it**




Base: 93 respondents (multiple responses permitted). Source: Pye Tait Consulting 2023.

'Other' sources were mentioned by seven respondents and included the following.

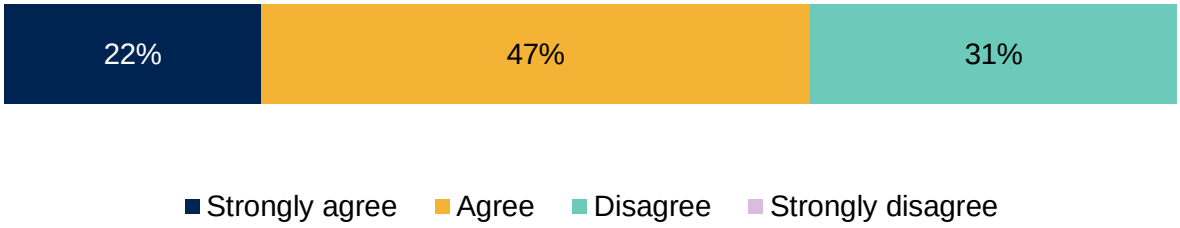
- Own general knowledge and research (four)
- NHS (one)
- Cyber Essentials Scheme (one)
- General Data Protection Regulation (GDPR) (one)

When an app store operator introduced the Code to an app developer, the majority said this happened prior to app submission, with very few saying it was afterwards (46% vs 7%). However, 46% could not recall the timing of this.

Those who were aware of the Code and who also said that an app store operator had signposted them to it, were asked to what extent they agreed that the information related to the Code of Practice provided by the app store operator was supplied in a way that was convenient and easy to access.

Around two thirds (69%) agree or strongly agree, while one third (31%) disagree – none strongly disagree.

**Figure 9 Extent information provided by app store operator on Code was convenient and easy to access**




Base: 32 respondents (those aware of Code and signposted to it by app store operator).
Source: Pye Tait Consulting 2023.

## 2.2 Engagement with and understanding of the Code

### 2.2.1 Raising awareness of the Code

Interviewed app developers were asked to what extent they feel further promotion is required to raise awareness of the Code among app developers.

Additional promotion is suggested by almost all (17 of 20), who feel the Code must be marketed and promoted further to have a significant impact on the industry. Six go on to discuss how the Code represents a chance to set guidelines and benchmarks for the industry to follow and to ensure a minimum standard of privacy and security, particularly as endorsed by government.

Eight propose the Code be disseminated via industry bodies. Holding tech conferences and having well-known developers and operators, such as Apple, Google, and Microsoft, promote the Code of Practice is also largely advocated. Six think the government should be the driving force, suggesting distributing information packs through social networks, or mandating best practice on development platforms.

Other suggestions to raise awareness of the Code of Practice, each noted by one interviewee, included the following.

- Developing an app for the Code, which reaches international developers and informs them of security and privacy requirements when developing apps for the UK market.
- Raising awareness among the base of potential clients.
- That any organisation which develops apps should be looking at the Code, given that apps can be developed 'at the drop of a hat'.
- Including the Code in university course content to inform students of their responsibilities.

Three suggest DSIT consider reviewing the Code's objectives, acknowledging that privacy and security requirements are crucial during app development. One suggests the Code could be mandatory in law instead of voluntary.

Widening the promotional scale of the Code to the global market was also seen to be useful by two, to help international developers acquaint themselves with UK privacy and security practices.

### 2.2.2 Accessibility of the Code

Interviewed app developers were asked how easy or difficult they found it to digest the information and principles within the Code of Practice, and whether the information should be conveyed differently.

Generally, the Code is described as straightforward and clear, with eight explicitly mentioning this point. In particular, the links to take readers to further reading on various aspects of the Code is appreciated.

However, three suggested the Code could be more interactive and visual, as opposed to mainly text in its current format. Creating alternative means of accessing the information within the Code is also proposed, for instance via video.

One participant feels the language caters more towards managerial staff rather than developers themselves and suggests more technical language is used in places. In contrast, another thinks the Code should be accessible to clients who are not familiar with technical jargon.

Two feel the Code is too long, and one notes a concise summary would be useful.

> *It gives me the information that I want, but I need to take notes on it to create a golden thread and understand exactly what it says. You have to spend time to digest it. Perhaps, a little bit more of a visual impact will be good for everybody. – Micro size firm, Yorkshire and the Humber, Aware of Code*

### 2.2.3 Content of the Code

Just under half of interviewees believe the Code to be comprehensive without gaps, i.e. there was nothing they were expecting to see that is not in the Code.

Gaps do exist according to others, detailed below.

- Instructions for how developers should test their apps against the Code's principles, either through internal or external mechanisms (three participants).
- A list of the likely consequences if an app does not meet certain principles (one).
- Accessibility guidelines should be included within the Code, with interviewees noting this is an aspect that forms a large part of other assessments for digital products (two).
- Detail on what to do in situations where an app is 'inherited' or passed on between developers (one).

A suggestion was put forward by one interviewee about the language used within the Code, for example the use of 'primarily applies to' might lead to the assumption that different principles are not relevant for certain developers, when, in fact, they are.

Staying abreast of technological developments means that the Code will need to be updated regularly.

## 2.3 Support required to adhere to the Code's principles

Surveyed app developers aware of the Code of Practice were asked what non-financial support (if any) would help them adhere to the principles contained in the Code, while those unaware of the Code were asked what non-financial support (if any) would help them adhere to a set of voluntary guidelines relating to app security and privacy.

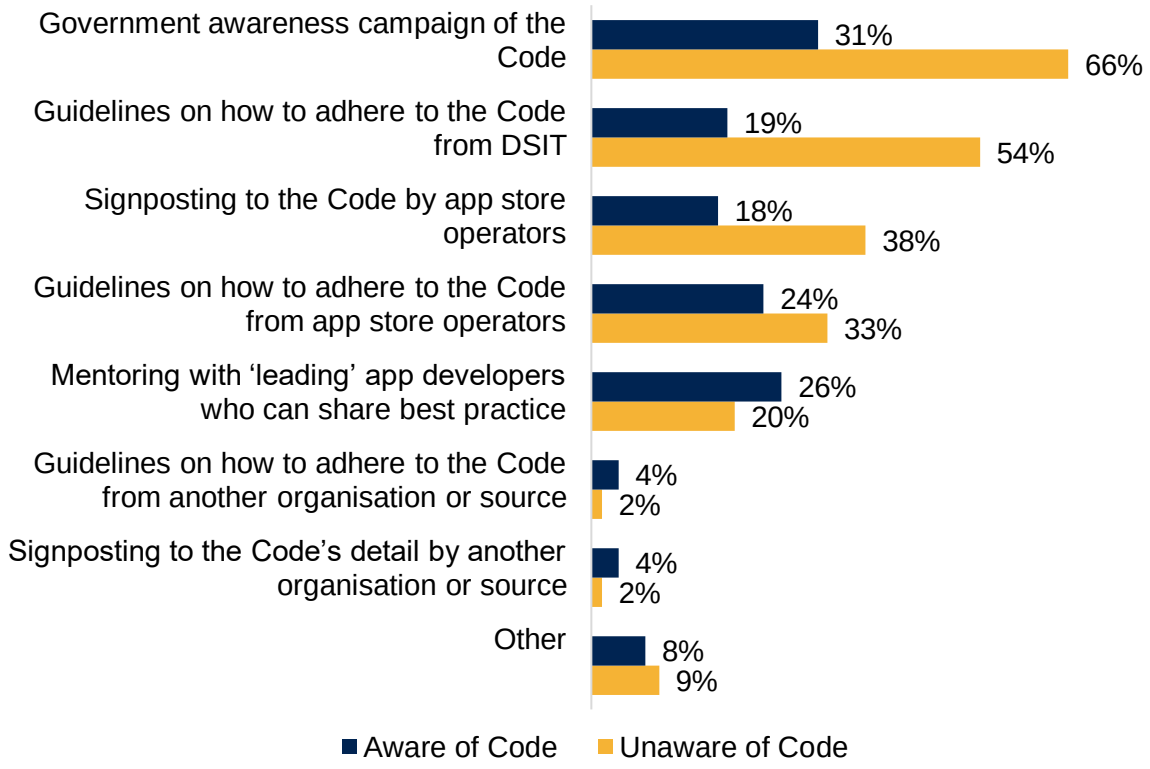
Those unaware of the Code typically ask for a greater degree of non-financial support.

The most common suggestion for support – from both those aware and unaware (mentioned by 31% and 66% of each group, respectively) – is for a government campaign to raise awareness of the Code.

Over half (54%) of those unaware of the Code would welcome some guidelines from DSIT on how to adhere to the Code, while around two in five (38%) would like signposting to the Code by app store operators, and one third (33%) would like guidelines on how to adhere to the Code from app store operators.

Of those aware of the Code, just over one quarter (26%) suggested mentoring with 'leading' app developers would be useful support, and just under one quarter (24%) would welcome guidelines from app store operators to help adhere to the Code's principles.

**Figure 10 Support required to help adhere to the Code's principles**




Base: 80 (aware) and 393 (unaware) respondents (multiple responses permitted).
Source: Pye Tait Consulting 2023.

'Other' suggestions for support to help to adhere to the Code's principles, or to a set of voluntary guidelines, were made by 45 respondents. Common suggestions include the following.

- A collaborative approach through forums and/or webinars (e.g. via chambers of commerce) to discuss principles with cyber security experts and government bodies (mentioned by eight respondents).
- Provision of examples of best practice and further guidance to make the Code/guidelines easier to understand. This could, for example, include a checklist and named points of contact for queries (seven).
- A central platform or website that app developers may refer to in order to access guidelines on implementing the Code/guidelines, including relevant legislation and examples (seven).
- Access to tech and legal experts who could provide advice on implementing the Code/guidelines (five).
- Further clarity on how the Code/guidelines will work in line with existing legislation, app store regulations and National Cyber Security Centre guidance (five).
- Support for testing against the Code's principles (three).
- Support for training and education, e.g. via courses or a specific initiative (three).

Among surveyed app developers unaware of the Code, there exist some differences of note.

- Significantly more micro and small app developers suggest a government awareness campaign would be helpful, compared to medium-sized firms (66% and 70% vs 22%).

- Those who develop apps for mobile and laptop/desktop platforms are significantly more likely to suggest support in the form of an awareness campaign (71% and 69% respectively), or guidelines from DSIT (both 60%), compared to those who develop apps for games consoles (48% – campaign, and 26% – guidelines).

- Compared to most UK regions, app developers based overseas are significantly more likely to suggest that mentoring with 'leading' app developers to share best practice would be useful support (48% of overseas app developers note this compared to 17% of UK-based app developers).

Interviewed app developers expanded on this, with five suggesting that access to mentoring and/or to a subject specialist would be helpful, for instance prior to/during implementing the Code to assess current practices and levels of adherence.

Four interviewees suggest that having available tools and/or guidance for testing adherence to the Code against current and ongoing practices internally would be useful, for instance in relation to how a breach should be exposed, or penetration testing kits available.

Examples of best practice are requested from three micro app developers, who would like to see best methods to implement the Code, published and endorsed by the government to provide weighting.

Greater industry engagement is suggested by three participants, for instance through the use of ambassadors, or through industry events.

### 2.3.1 Ease of implementation

Just under half of interviewees envisage they would have no issues implementing the Code, as their existing processes and procedures already align to the principles within the Code.

Three discussed the costs associated with implementing the Code that could cause difficulties for implementation, including for providing relevant training and hiring new developers. One highlighted that the Code could cause difficulties for new businesses as they might not be able to afford to meet the standards. (See section 2.4 for more detail on costs of implementation.)

Two found it difficult to comment on this, pointing out this will depend on multiple factors, including the current success of the business and how quickly existing processes are adapted to integrate the Code's principles before it is a requirement.

Some form of incentive is suggested by one developer, noting that it will be difficult to engage with developers without them having a tangible incentive to do so.

## 2.4 Cost of implementation

Thinking of the time and job roles in their business, surveyed app developers were asked to provide approximate costs of implementation, in relation to costs that would not otherwise be incurred were it not for having to adhere to additional guidelines. These were gathered on a 'per organisation' basis (rather than on a 'per app' basis).

Those aware of the Code were asked for costs associated with implementing the Code for their organisation, while those unaware were asked about costs associated with implementing a set of voluntary guidelines for their organisation relating to app security and privacy for developers. It should be noted that many respondents (around 54% of those aware of the Code, and 76% of those unaware of the Code) felt unable to provide a response.

**Table 5 Average (mean) estimated cost of implementation**

| Aspect | Aware of Code | Unaware of Code |
|---|---|---|
| Familiarisation | £7,143 | £3,343 |
| Scope, develop, test, and implement new/revised processes required to adhere to the requirements | £18,882 | £2,906 |
| Legal costs | £4,374 | £654 |
| Other costs | £217 | £414 |

Base (top to bottom): 43, 43, 42, 6 (aware) and 136, 118, 124, 40 (unaware) respondents.
Source: Pye Tait Consulting 2023.

Of those who could provide an estimated cost, the most common (modal) cost given for each aspect is zero. A zero figure was given by around 40% to 50% of surveyed app developers; for both those aware and those unaware of the Code. This would indicate that around half of surveyed app developers see no additional cost for them in having to adhere to principles contained in the Code.

The average (mean) cost estimated is typically higher among those aware of the Code than among those unaware of the Code. This is likely due to such developers already holding awareness of what the Code comprises and what actions are required. It may also be a reflection of the fact that more larger firms are aware of the Code, resulting in a greater cost estimate.

For those who estimated there would be a non-zero cost, responses (combining estimates from both those aware and those unaware of the Code) ranged from £3 up to £300,000 with a small number of larger estimates skewing the overall average (mean). As an example, one business responsible for a well-known and popular mobile app in the UK provided an estimate of £112,000 for annual costs for penetration testing, and a further £145,000 annual costs to host their client's app, in accordance with the Code.

For those aware of the Code, responses typically (though not exclusively) range between £500-£5,000 for familiarisation and again for legal costs, and between £1,500-£10,000 for

scoping and developing aspects. The median costs for familiarisation, legal, and scoping/development are £300, £5, and £500, respectively.

For those unaware of the Code, responses typically (though not exclusively) range between £100-£5,000 for familiarisation and again also for legal costs, and between £200-£10,000 for scoping and developing aspects. The median costs for familiarisation, legal, and scoping/development are £200, £0, and £200, respectively.

'Other' costs mentioned typically related to insurance, staff recruitment and retention and development activities, as well as software and tools required, and knowledge sharing through engagement and outsourcing activities.

Readers should bear in mind when interpreting these figures that there is a degree of uncertainty as to whether these represent short-term or ongoing costs (or potentially both). Further, it is unclear whether these costs are scalable (e.g. by size of business).

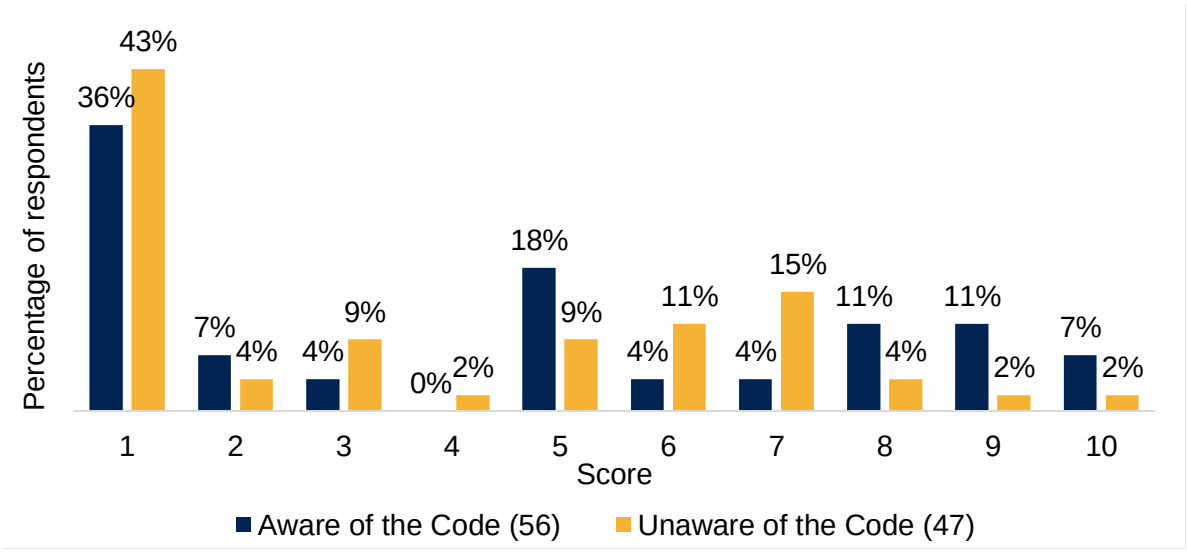
### 2.4.1 Impact of costs on business

For those aware of the Code, the average (median) rating of the impact of the costs associated with implementing the Code on their business was five (on a scale from one (no impact at all) to 10 (very significant impact)).

For those unaware of the Code, the average (median) impact of the costs associated with implementing a set of voluntary guidelines relating to app security and privacy on their business was three (on the same scale).

The most common (modal) response in both instances was one, with around two in five indicating that the associated costs would have no impact. Other responses are spread towards the mid to higher end of the scale, with these app developers indicating there would be some moderate impact.

**Figure 11 Extent that costs associated with implementation might impact business**




1 = no impact at all, 10 = very significant impact. Source: Pye Tait Consulting 2023.

Respondents were asked to explain their answer and 84 comments were received. Scores have been grouped into three bands to outline themes among different groups, with 48 comments for the band of rating one to three, 25 comments for a rating of four to seven, and 11 comments for a rating of eight to 10. These small sample sizes mean findings should be treated with caution.

### Rating of one to three (low to no impact)

Some (15, 16%) highlighted that their existing internal practices meet the requirements of the Code, and therefore will not incur any additional cost. This is because app developers wish to follow their own processes which they feel are sufficiently robust, with two stressing the Code is voluntary.

Others (11, 12%) said they refer only to app store operators' guidelines and note that their compliance is based on operators' requirements as they are continuously updated. Mobile app developers name the Apple App Store and Google Play specifically. One highlights the similarity of the Code and current requirements of app stores in general:

> *The Code is basically already what the app stores rigorously enforce. So the cost of compliance to the Code is the same as the cost of being compliant with the app stores on each application. – Medium size firm, London, Aware of Code*

A few (five, 5%) said they have no intention to implement the Code, and therefore will not incur any additional cost to their business. A couple (2%), however, anticipate that they will use the Code as guidelines for future development.

A few (five, 5%) stated that any cost of implementing the Code would be passed to their clients.

### Rating of four to seven (some impact)

Some (nine, 9%) mentioned that the greatest cost associated will be time. This includes the time taken to ensure the Code/guidelines are met, to conduct the relevant work and for developers to implement.

A few (four, 4%) reported that the upfront costs required to implement the Code have had/will have the greatest impact. One small and one micro business discussed how the cost might be too great, meaning they would be unable to recoup this.

A couple (two, 2%) mentioned they have no intention to implement the Code and will be following app store operators' guidelines, and therefore see limited impact.

Potential increased costs due to involving freelancers, the need for training, or increased trading costs are each mentioned by one respondent (1%).

### Rating of eight to 10 (high impact)

A few (three, 3%) simply stated that the costs associated with implementing new procedures or adapting current practices would be very high.

A handful (three, 3%) pointed out how the costs associated with regularly updating apps in compliance with the Code/guidelines are difficult to predict and will likely be high, especially with monitoring requirements.

This topic was further explored with interview participants. Two in five anticipated that implementing the principles within the Code will not result in extra costs and will therefore not financially burden their organisation. They each highlight that their current processes cover the principles within the Code and will not require any further work to be compliant.

> *There will be no financial burden for us. I think it's something that my developers need to be mindful of, and we do have our own procedure for doing this. But also, from a legislative point of view, they need to be aware of what's out there that is mandating what's happening. – Small size firm, Scotland, Aware of Code*

Five app developers (comprising both those aware and those unaware of the Code, and different company sizes) referred to the time cost required to implement the Code. One micro company suggested it might take them up to a year to review their current processes and systems.

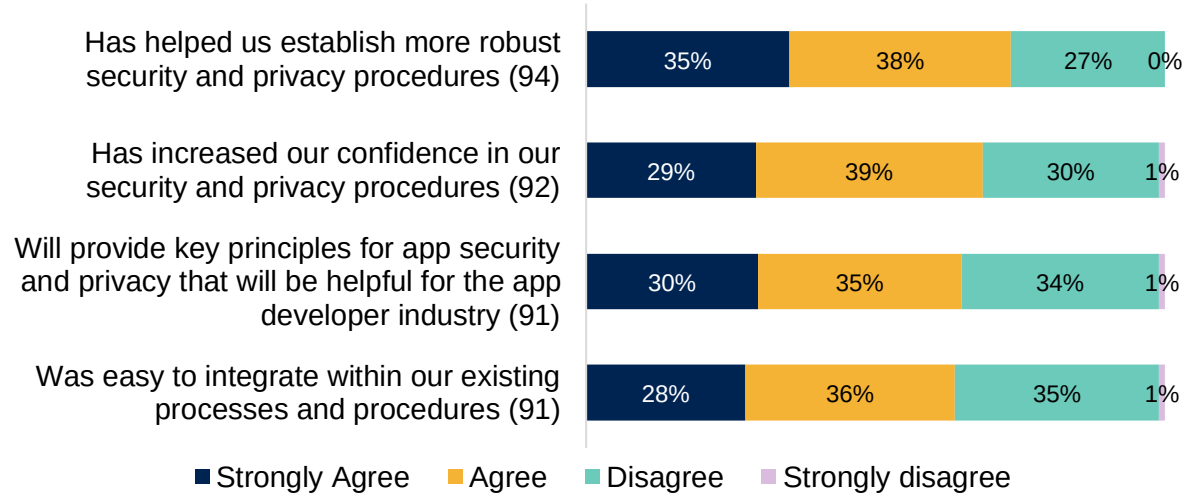
Three mentioned the cost of redevelopment, particularly in instances where apps do not currently adhere to the Code, and there would be a greater cost if an app needed stripping back to re-work from the foundations.

Three said they would need to hire more staff to monitor their compliance with the Code, noted by micro, small and medium businesses, but with a potentially greater relative impact for smaller app developers.

## 2.5 Influence and impact of the Code

The 16% of surveyed app developers aware of the Code were asked for their views in relation to certain aspects of its impact. Around two thirds agree or strongly agree with each presented statement, with agreement highest in relation to the Code helping to establish more robust security and privacy procedures (73%) and lowest – but still reasonably high – that it was easy to integrate within existing processes and procedures (64%).

**Figure 12 Views on the Code among app developers aware of it**



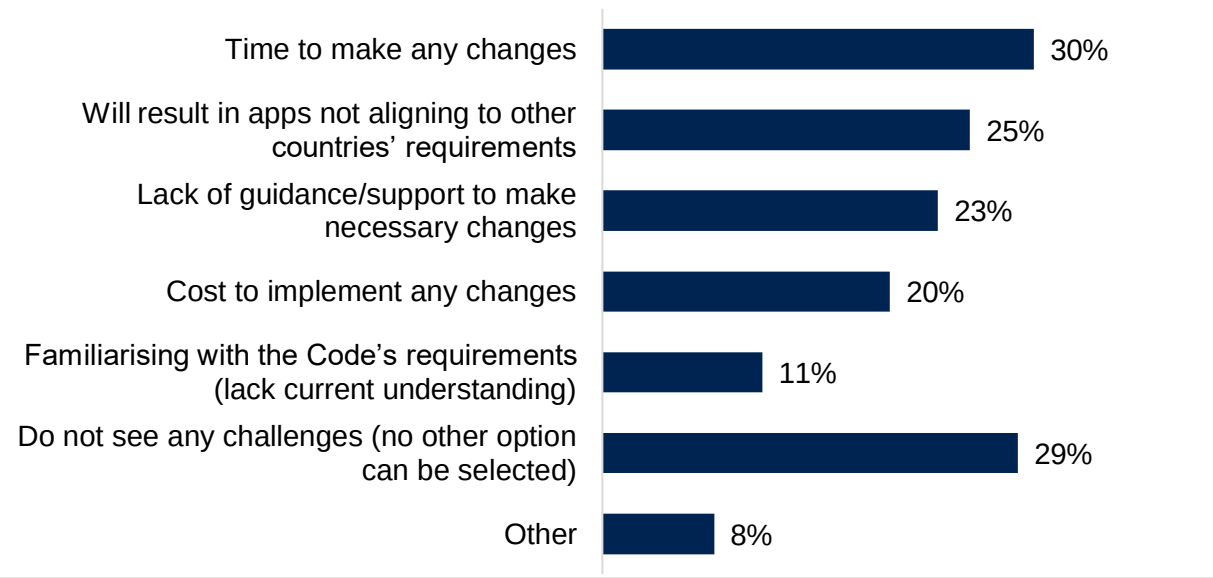

Source: Pye Tait Consulting 2023.

There were no significant differences in levels of agreement by region, platform, or size of company.

The main challenges among those aware of the Code in implementing/aligning to the Code revolve around time to make changes (30%), a concern that this may result in apps not aligning to other countries' requirements (25%), a lack of guidance or support (23%), and cost (20%).

Just under three in ten (29%) see no challenges.

**Figure 13 Perceived challenges to implement/align to Code (among those aware of it)**




Base: 91 respondents (multiple responses permitted). Source: Pye Tait Consulting 2023.

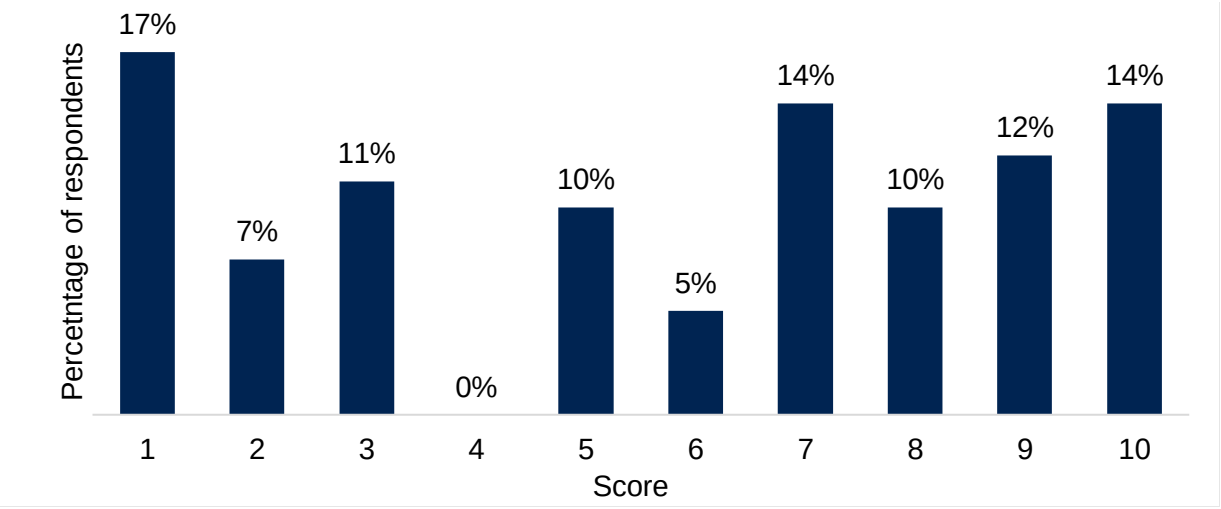
'Other' challenges mentioned included the following.

- There are other requirements (e.g. clients' needs) to also align to (noted by two respondents).
- Sharing knowledge with development team (one).
- Getting qualified staff (one).
- Apple's requirements reportedly vary on what can/cannot be used on platforms (one).
- Restrictions not having to reduce functionalities (one).

Surveyed app developers based overseas are significantly more likely to note that implementing or aligning to the Code will result in apps not aligning to other countries' requirements (noted by 63% of such) compared to app developers based in most other UK regions.

Those aware of the Code provided an average (median) rating of seven in terms of the Code's impact on their security and privacy processes – on a scale from one (no influence) to 10 (highly influential). The most common (modal) response – noted by one in six (17%) – is one, however, half (50%) score at seven or higher and just over one quarter (26%) scoring nine or 10, indicating the Code has had an impact.

**Figure 14 Extent of Code's influence on security and privacy practices (among those aware of it)**




1 = no influence, 10 = highly influential. Base: 83 respondents. Source: Pye Tait Consulting 2023.

The average (median) score of medium sized app developers (nine) is significantly higher than that of micro and small companies (six and five, respectively). Large firms also score highly (nine median average) showing the Code's influence would appear to scale by app developer size.

The Code's influence is also significantly higher for developers of apps for wearable devices (median of 10), voice assistant platforms (10), and smart TVs (nine) compared to those developing apps for laptops/desktops (six).

Asked to explain their answer, 49 provided comment. Some (six, 12%) of those scoring between one and three feel that app store operator guidelines take priority over the Code of Practice, while a few (three, 6%) feel internal developer company guidelines take priority over the Code. A couple (two, 4%) believe the Code does not apply to them as they develop apps for the international market.

Of those scoring between four and seven, several (six, 12%) described the Code as useful, to some degree. A few (three, 6%) pointed out that the utility of the Code is dependent upon clients/user base. A similar number (three, 6%) in this group also felt that app store operator guidelines take priority over the Code of Practice.

Several (six, 12%) of those scoring between eight and 10 mentioned the importance of following guidance set out by the UK Government, particularly when working on security and privacy matters, noting the Code has been helpful in this regard. The necessity of following guidelines in general, to ensure client satisfaction or maximise the likelihood of app publication, is also commonly discussed (six, 12%).

### 2.5.1 The Code's impact on app developer's growth in UK market

Interviewed app developers were asked to what extent they feel the Code might influence their organisation's growth in the UK market. Just under half feel the Code will have a positive impact for their business' growth, whilst around one in three explicitly state it will have no impact.

The introduction of an accreditation or 'badge' to demonstrate compliance with the Code is suggested by 12 participants as a method to increase the likelihood of the Code positively influencing their businesses growth. This will, it was argued, allow developers to advertise their compliance to customers and provide further security confidence for clients. Two furthered this by noting the Code will emphasise the developers' commitment to secure processes and strengthen the companies' reputations to build trust with current and future clients.

> *If there's accreditation, that would put us above competitors, [to show] we do adhere to accessibility standards or GDPR standards or whatever it may be. – Medium size firm, London, Aware of Code*

Two noted that the influence of the Code will be determined by the awareness of it within the industry: if the industry is not aware, it is likely that other developers and clients will be ambivalent towards it.

However, two say compliance with the Code is expected to increase opportunities for success with contracts and tenders as developers anticipate this becoming a selection criterion for government work in future.

# 3. Current security and privacy practices

This chapter examines app developers' current approaches to security and privacy matters, and the extent to which these align to the Code's principles.

## 3.1 General approach to security and privacy

Interviewed app developers were asked about the main security and privacy practices they always implement when developing apps. The majority (14) discussed encryption in this regard and mostly in reference to storing and processing personal data. Some mentioned specific methods and third-party services that they use including Advance Encryption Standard (AES) 256, Statistical Analysis System (SAS) platforms, and Cryptographic Message Syntax (CMS).

Eight discussed access to personal data, noting how their apps are designed so that only necessary personal data are recorded or stored to minimise the risk of potential security issues. One mentioned that their app users are offered a simple method to view a record of their personal data, and to request its deletion.

Six commented on data storage to outline how personal data are kept secure. Three elaborated how they use third party software and services that they believe offer maximum security, including Amazon Web Services (AWS) cloud and Stripe. One noted how it ensures unnecessary data are removed from data caches, as these are vulnerable to attacks and breaches.

Five also pointed out how they ensure all passwords and logins are secure, for example via hashing and encryption of passwords, and implementing processes such as two-factor authentication.

Five (of which all develop apps for mobiles) outlined how they have simple uninstall processes, while others discussed how they have processes to update and fix vulnerabilities should they appear.

Other security and privacy practices regularly implemented include constant testing during development (three), penetration testing (two), and referring to available guidelines (including GDPR and app store operators') (three).

### 3.1.1 Drivers in adopting practices

Several (seven) stated there is a commercial incentive for adapting these security and privacy practices – the development of rigorous security practices is expected by potential clients, and ensuring this allows for more success in winning contracts.

> *Nowadays you have to have a fairly safe and secure application if you want to compete within the marketplace. Some of our customers are corporate customers and this is amongst their requirements - they expect it. – Micro size firm, South West, Unaware of Code*

Risk was also flagged as a driver by seven interviewees – both the risk of a data breach itself on their companies' systems and the damage this could cause, as well as the potential reputational damage of such an occurrence.

Indeed, six agreed that there is a moral incentive to adapt such practices, with recognition that apps have the potential to be exploited if not sufficiently protected – they feel morally obliged to ensure the robustness of their security and privacy practices as it is in the best interest of their clients and users.

Six interviewed app developers previously unaware of the Code of Practice stated that regulation and legislation would drive their security and privacy practices.

Three also commented that quality is a fundamental incentive, with a desire to produce a high-quality product.

### 3.1.2 Frequency of updating apps

There is some variance in how frequently interviewed app developers update their apps, from weekly to quarterly, with a handful doing so annually. Many noted that timeframes for updates can vary, depending on a variety of factors, such as the nature of the update, the device the app is being updated for, and the operating system the app is designed for.

Several (eight) discussed how they update their apps in the event of a potential vulnerability. Such updates are generally more urgent and implemented in a shorter timespan than a more general update.

> *Some [updates] are event-driven so if there is a problem we just go through it, all hands on deck and fix and launch the update. – Small size firm, South East, Aware of Code*

On the other hand, some developers will update apps for the sake of improved functionality (four) or fixes (three). These updates, not being security-related, are non-urgent and occur to a fixed schedule.

A few (four) noted particularities in operating systems and app store operators.

- Android apps are updated more frequently than Apple apps (3 months vs 12 months).
- App store operators may contact developers regarding issues with an app, which affects their update schedule.
- Apple App Store will stop facilitating an app if it is not updated frequently enough (two to three times per year).

In addition, one stated that its smart television apps are updated less frequently than their mobile apps, as they have fewer features and do not store personal data.

## 3.2 Alignment to Code's principles

This section outlines app developers' current security and privacy practices, and the extent to which these align to the principles contained in the Code. It also explores whether app developers have an organisational plan in place to align to these principles, and – if not – the reasons for this.

### 3.2.1 Current security and privacy practices

Surveyed app developers were asked about the extent to which they undertake various security and privacy practices. These practices align directly to the principles within the Code of Practice, although this was not brought to respondents' attention.

Over four in five surveyed app developers said that, for all apps they develop, they undertake certain practices.

- Take steps to ensure their app adheres to minimum security and data protection requirements (86%).
- Provide updates to fix security vulnerabilities (85%).
- Use industry standard encryption (84%).
- Have a process to readily update and monitor their software dependencies in all published versions of an app (82%).

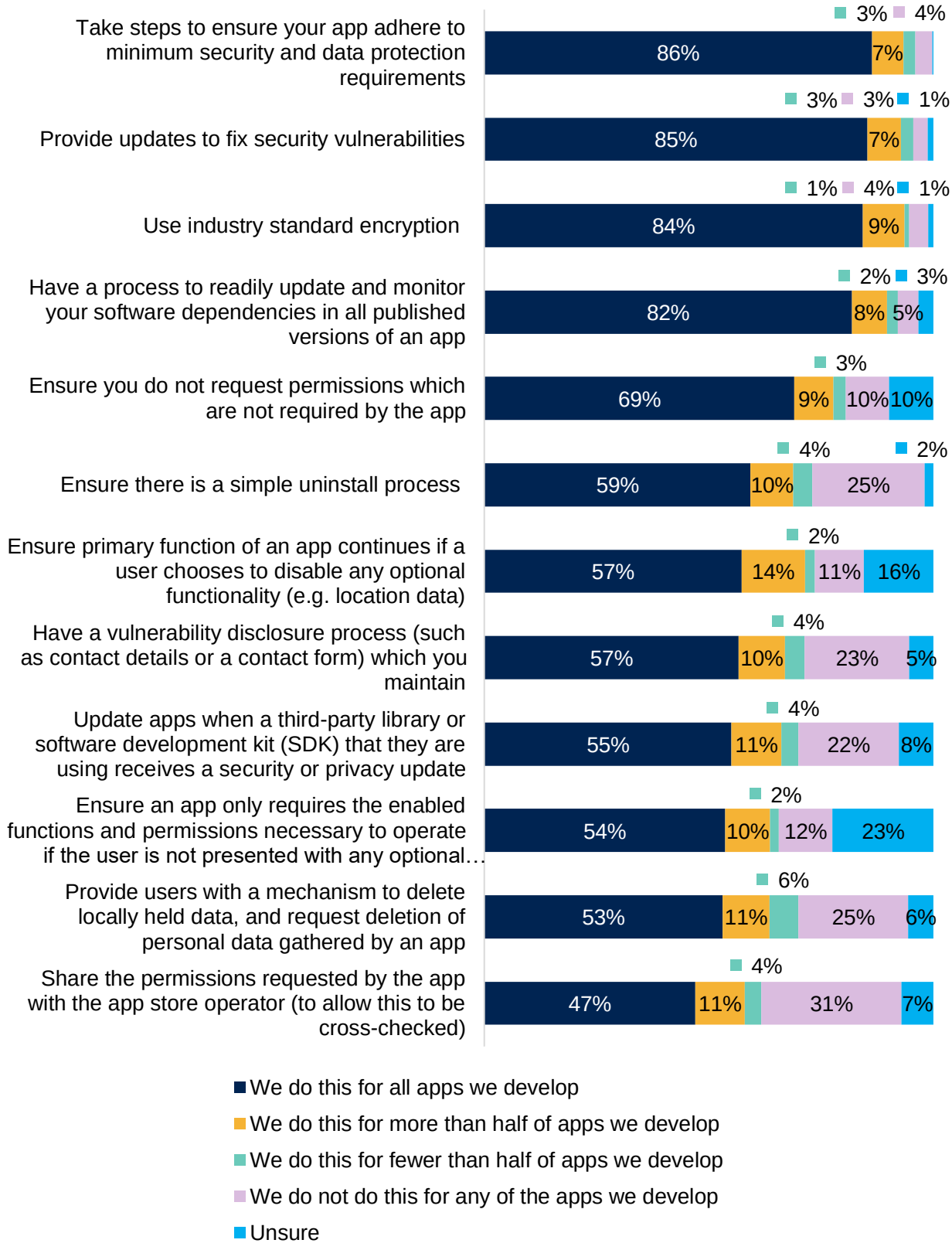
Under half (47%) said that, for all apps they develop, they share the permissions requested by the app with the app store operator (to allow this to be cross-checked).

Almost all other security and privacy practices asked about are undertaken by between 53% and 59% of surveyed app developers for all apps they develop.

Meanwhile, at least one quarter said they do not do the following for any apps they develop.

- Share the permissions requested by the app with the app store operator (to allow this to be cross-checked) (31%).
- Ensure there is a simple uninstall process (25%).
- Provide users with a mechanism to delete locally held data, and request deletion of personal data gathered by an app (25%).

**Figure 15 Security and privacy practices currently used**




Base: varies from 586 to 599 respondents. Source: Pye Tait Consulting 2023.

Surveyed app developers who develop apps for smart TVs, games consoles, or voice assistant platforms, were significantly more likely to undertake the following practices for all or over half the apps they develop, compared to those developing apps for mobile or laptops/desktops.

- Ensure there is a simple uninstall process.
- Share the permissions requested by the app with the app store operator (to allow this to be cross-checked).

Similarly, surveyed app developers aware of the Code were significantly more likely to undertake the following practices for all or over half the apps they develop, compared to those unaware of the Code.

- Ensure the primary function operates if a user chooses to disable any optional functionality.
- Ensure an app only requires the enabled functions and permissions necessary to operate if the user is not presented with any optional functionalities.
- 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).
- Ensure there is a simple uninstall process.
- Provide users with a mechanism to delete locally held data, and request deletion of personal data gathered by an app.
- Update apps when a third-party library or software development kit (SDK) that they are using receives a security or privacy update.

### 3.2.2 Organisational plans in relation to security and privacy

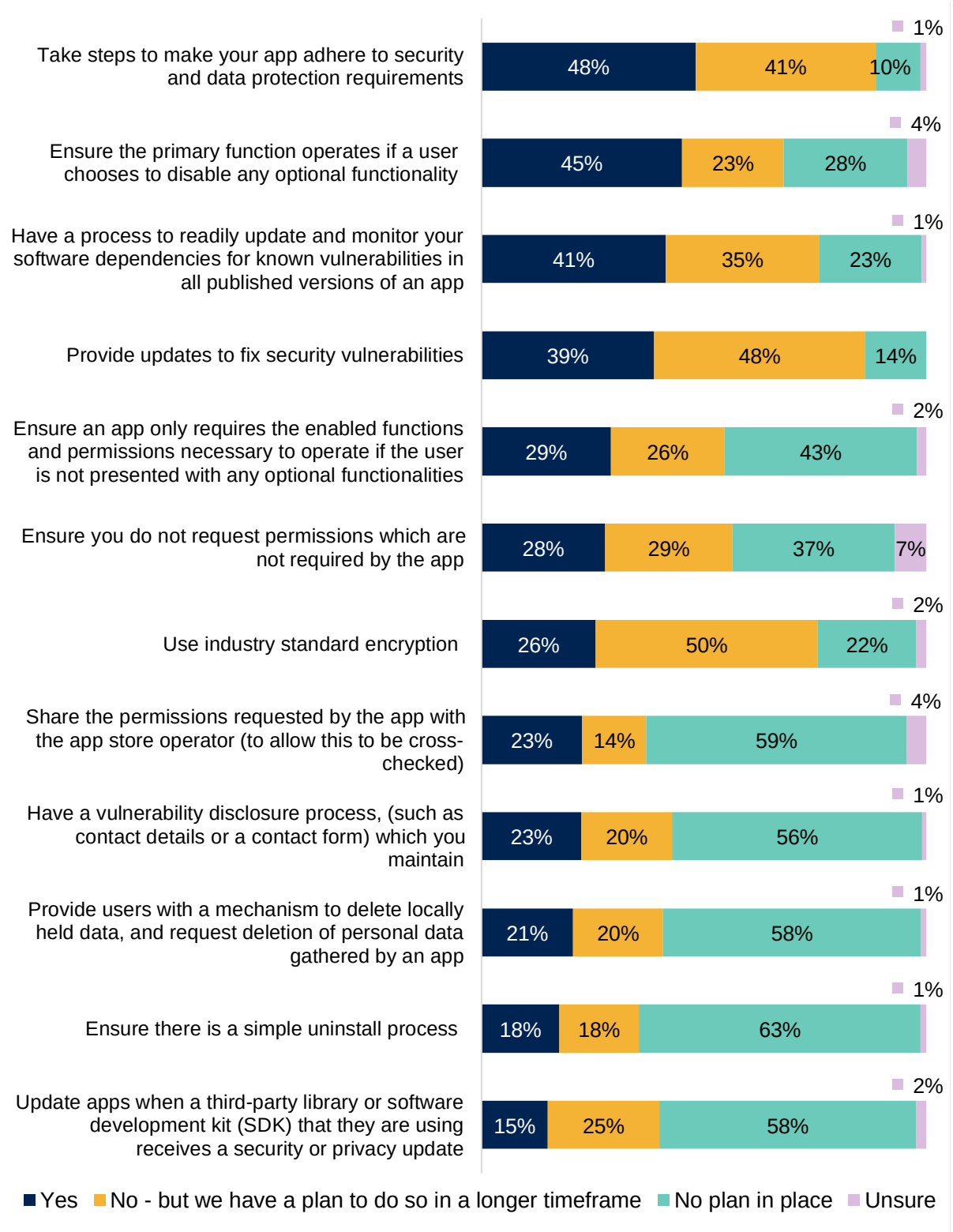
In cases where developers said not all their apps align to certain security and privacy elements, under half said they had an organisational plan in place over the next 12 months for each element, ranging from 48% saying they plan to take steps to ensure their app adheres to minimum security and data protection requirements, to 15% who say they will update apps when a third-party library or software development kit (SDK) that they are using receives a security or privacy update.

However, a sizeable proportion do have plans in place to implement some elements, but over a longer period of time, for example using industry standard encryption (50%), and providing updates to fix security vulnerabilities (48%).

For several elements, however, over half of surveyed app developers highlighted that they have no plans in place to implement certain practices.

Surveyed app developers who were aware of the Code were significantly more likely to say they had a plan in place to implement such security and privacy practices within the next 12 months than those who were unaware of the Code, for eight of the 12 elements in question.

**Figure 16 Whether organisational plan in place to implement security and privacy practices**




Base: varies from 79 to 270 respondents. Source: Pye Tait Consulting 2023.

### Rationale for not having an organisational plan in place

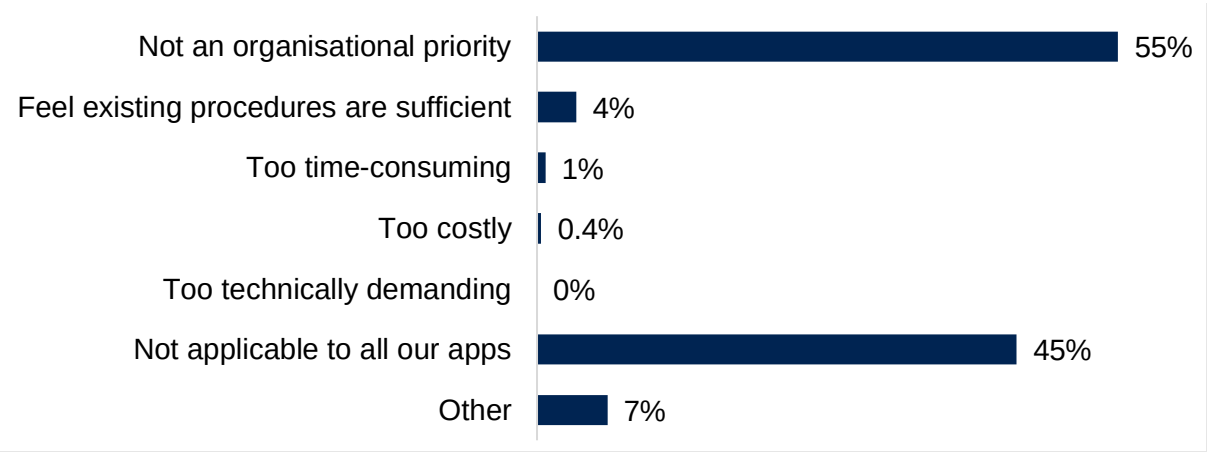
Surveyed app developers who stated they had no plan in place for at least one element most commonly (55%) put this down to not being an organisational priority.

Meanwhile 45% did not feel the element was applicable to all the apps they develop – asked to expand on this, 104 comments were received, with one in three of these (34, 33%) saying they develop bespoke apps that are just for the business purposes of a given client, meaning that some procedures such as uninstallations and regular software updates are not relevant. A similar proportion (33, 32%) said their apps are not available on any app stores for public use, so some elements such as sharing app permissions with an app store operator are out of scope.

> *It is not relevant to what we do. Our apps are bespoke made, you cannot download them from app stores. – Micro size firm, Scotland, Unaware of Code*

Several (25, 24%) noted some of their apps are web-based and not available on mobile devices, therefore certain practices, such as uninstall processes, are not relevant. Others (16, 15%) stated that security practices were not applicable because their applications do not collect or store personal data.

**Figure 17 Reasons why no plan in place to implement security and privacy practices**




Base: 242 respondents (multiple responses permitted). Source: Pye Tait Consulting 2023.

'Other' reasons were mentioned by 16 respondents and most commonly mentioned are as follows.

- The app only stores and processes anonymous, non-personal data (four).
- Security and privacy practices are covered by other platforms such as Microsoft (four).
- The app developer only enhances the app and advises on questions concerning different features, while the client handles permissions and security (two).

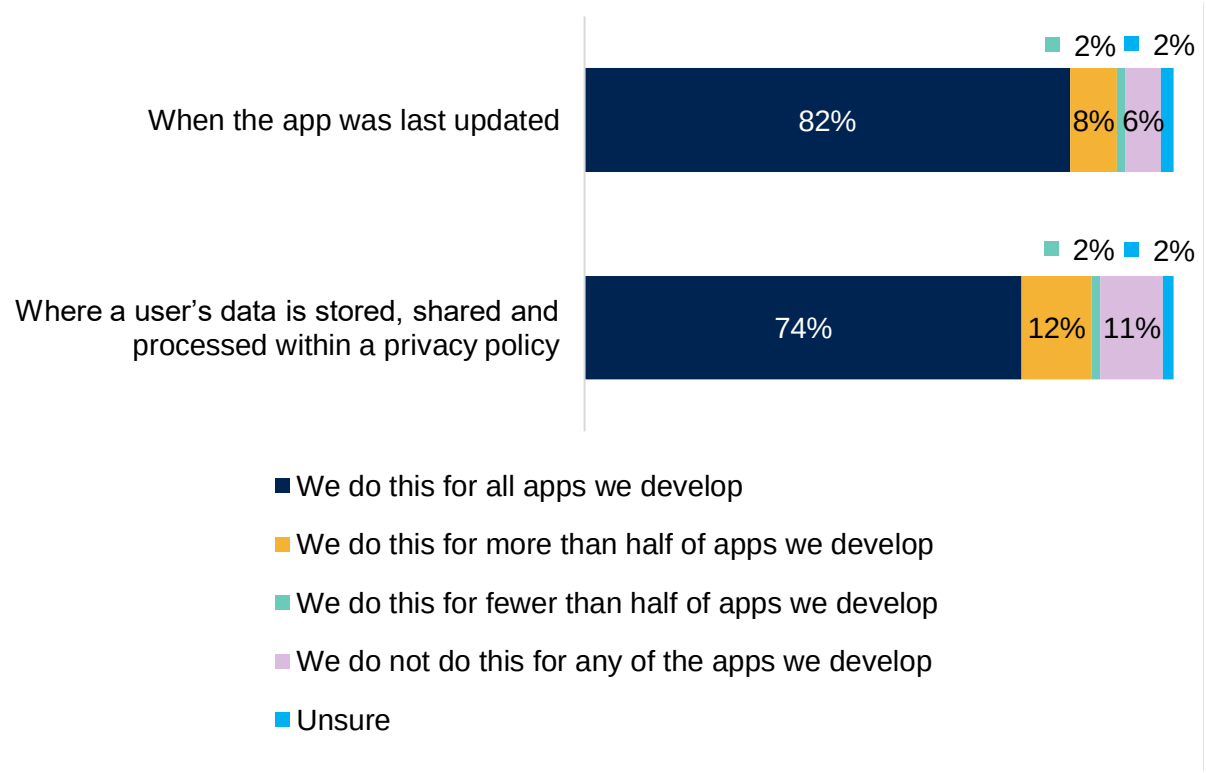
A significantly higher proportion of surveyed app developers unaware of the Code said that they had no plan in place as this was not an organisational priority, compared to those who were aware of the Code (59% vs 17%).

### 3.2.3 Provision of information, and reacting to personal data breaches

Surveyed app developers were also asked whether they provided information about the behaviour of apps they develop – again these points align to some of the principles in the Code of Practice, but this was not noted to respondents at this point.

Over four in five (82%) said that, for all the apps they develop, they provide information about when the app was last updated. Just under three quarters (74%) say they provide information on where a user's data is stored, shared and processed within a privacy policy, for all apps they develop.

**Figure 18 Extent to which app developers provide certain information**




Base: 598 (top) and 596 (bottom) respondents. Source: Pye Tait Consulting 2023.

For both elements, a significantly higher proportion of those aware of the Code provide such information for all or over half the apps they develop, compared to those unaware of the Code.

In addition, some surveyed app developers (48 in total) said they provide some additional relevant security information for at least some of the apps they develop and expanded on

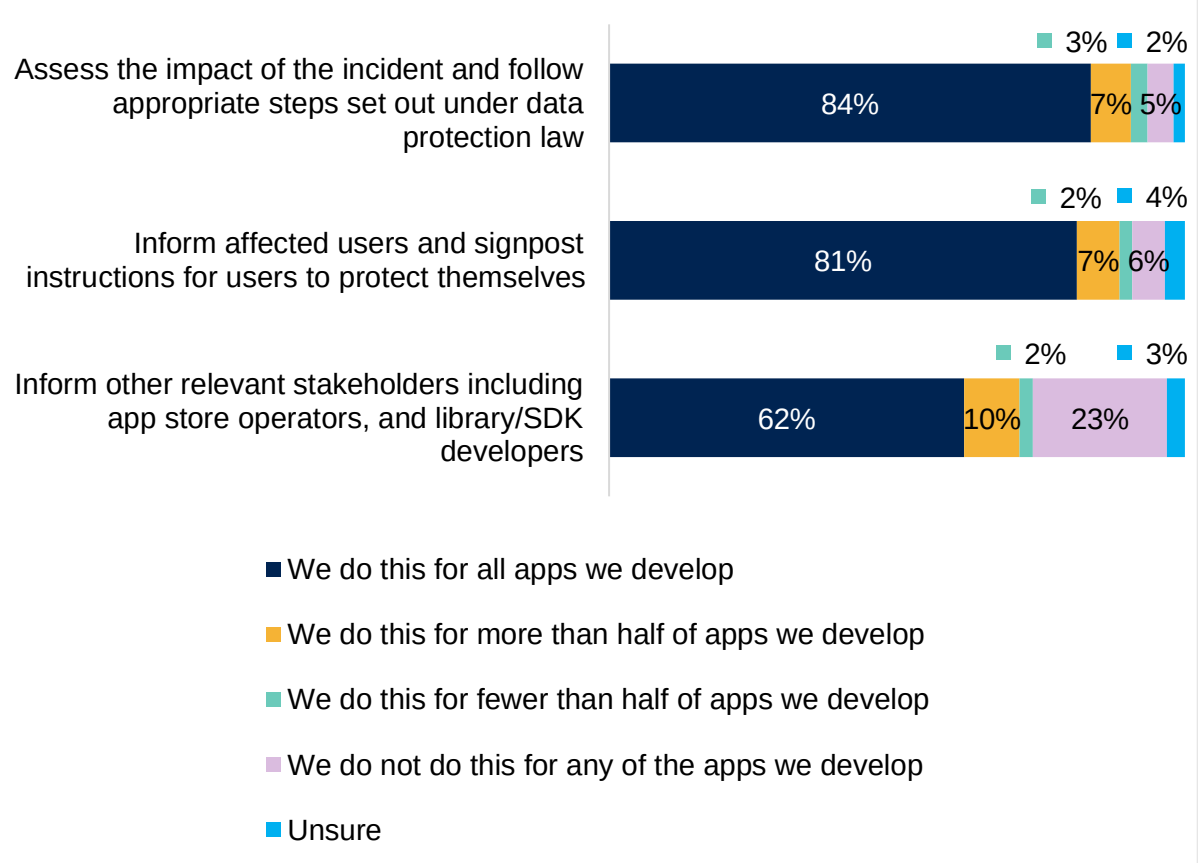
what such information included. Examples commonly given included extra security protocols (particularly in instances where processing large volumes of personal data), or further information tailored to client's bespoke requirements. Three also say they provide password encryption, and one provides a best practice user guide for security and privacy.

Surveyed app developers were further asked to what extent they would undertake certain activities if they became aware of a security incident involving a personal data breach in one of their apps. Once again, these activities align to the principles in the Code of Practice, but respondents were not made aware of this.

Over four in five said that, for all apps they develop, they would assess the impact of the incident and follow appropriate steps set out under data protection law (84%), or inform affected users and signpost them to instructions to protect themselves (81%).

Around three in five (62%) would inform other relevant stakeholders for all apps they develop, although around one quarter (23%) would not do this for any apps they develop.

**Figure 19 Extent that certain activities would be undertaken if app developer became aware of a personal data breach**



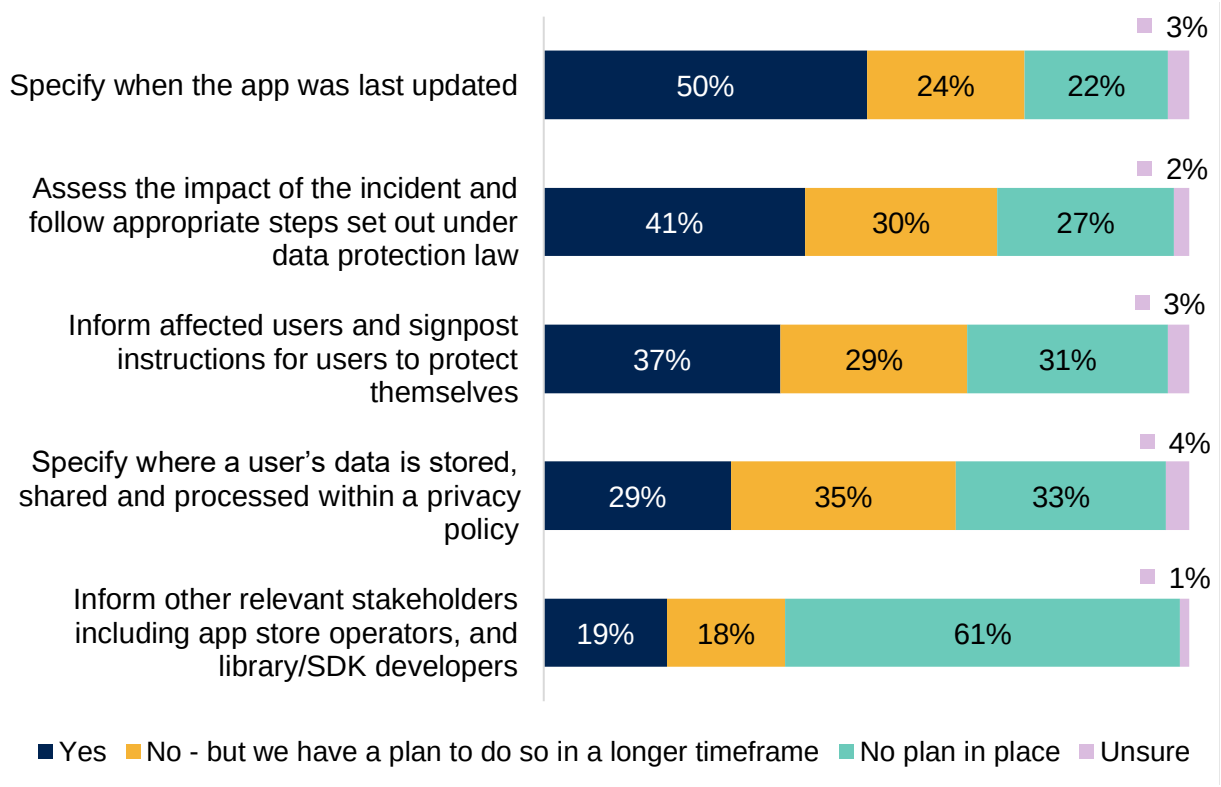

Bases (top to bottom): 596, 595, and 594 respondents. Source: Pye Tait Consulting 2023.

Significantly more of those aware of the Code would inform other stakeholders for all or over half the apps they develop, compared to those unaware of the Code (90% vs 68%).

## Organisational plans in relation to security and privacy practices

Where respondents indicated that they did not undertake certain activities for all the apps they develop, half (50%) plan, in the next 12 months, to specify when the app was last updated, and just over two in five (41%) similarly plan to have in place procedures to assess an incident's impact. Just under one fifth (19%) plan to have procedures in place to inform other stakeholders – indeed just over three in five (61%) say they have no plans in this regard.

**Figure 20 Whether organisational plan is in place to implement security and privacy practices**




Base: varies from 84 to 209 respondents. Source: Pye Tait Consulting 2023.

For all practices, those aware of the Code are significantly more likely to have a plan in place over the next 12 months to implement such practices, compared to those unaware of the Code (with the exception of specifying where a user's data is stored, shared and processed).

## Rationale for not having an organisational plan in place

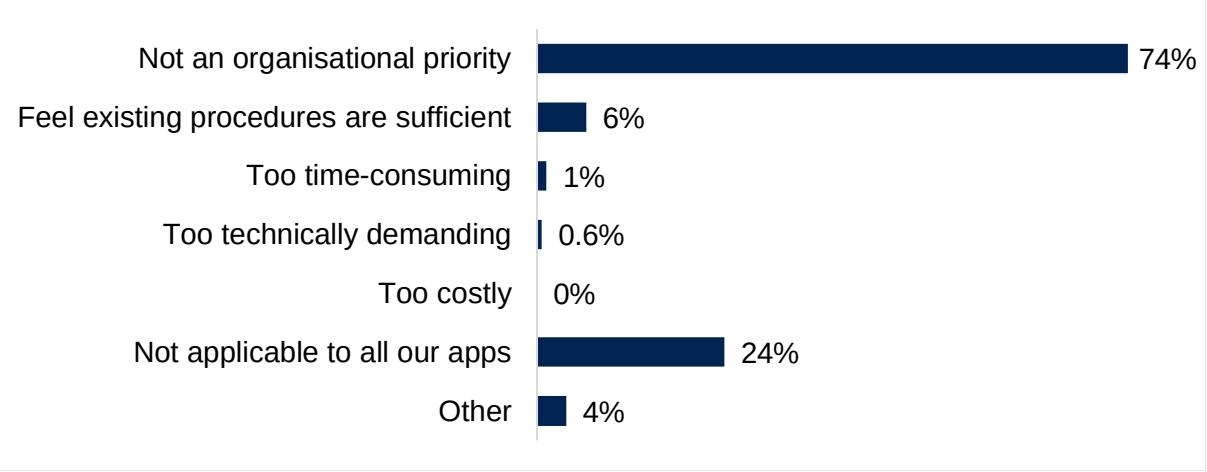
Surveyed app developers who stated they had no plan in place for at least one element most commonly (74%) put this down to not being an organisational priority.

Meanwhile, just under one quarter (24%) did not feel the element was applicable to all the apps they develop, with 34 respondents providing further comments. Several of these (13, 38%) noted that such apps may not store or collect personal data.

> *There is no need or requirement for vulnerability disclosure, our apps do not store any personal data – Micro size firm, North West, Unaware of Code*

Some said they do not use any app stores as the apps they develop are tailored for business use (seven, 21%), while others (10, 29%) say some of their apps are web-based.

**Figure 21 Reasons why no plan in place to implement security and privacy practices**




Base: 162 respondents (multiple responses permitted). Source: Pye Tait Consulting 2023.

'Other' reasons were mentioned by six respondents.

- Such aspects are the client's, not the app developer's, responsibility (three).
- Use a disclaimer and signposting to other links currently which is felt to be sufficient (two).
- Moving away from mobile apps to website and digital design (one).

A significantly higher proportion of surveyed app developers unaware of the Code said that they had no plan in place as this was not an organisational priority, compared to those who were aware of the Code (76% vs 40%).

## Reacting to a personal data breach

In the event of a personal data breach in an app they develop, interview participants said they would most commonly notify users of their apps (mentioned by 11 interviewees) and the Information Commissioner's Office (ICO) (seven), with some also saying they would inform clients (five), their internal staff (four), and app store operators (two).

> *The moment that we become aware of a data breach, the clock is ticking. When we internally define what has happened, we will formally notify this business and then the ICO. – Micro size firm, Yorkshire and The Humber, Aware of Code*

Five have in place an internal policy if such a breach were to occur, although two say they do not have such a company policy – one develops gaming apps which do not involve personal data, while another said they knew the "rough path" to follow.

Five interviewed app developers pointed out that the responsibility of notifying relevant affected parties would fall to their clients who own and manage the apps developed for them.

Interview participants were further asked what level of information or guidance they would provide in the event of a personal data breach in an app they develop. Seven stated they would provide specific information to parties involved in the breach, including: what data had been breached, when the breach occurred, and what steps were being taken to remedy the situation.

> *We would disclose all information, what information we hold on them, what has been exposed, and what our internal steps/measures will be. – Small size firm, North West, Unaware of Code*

On the other hand, two said they would be less keen to disclose information, with one explaining how they would notify relevant parties that such an event occurred but not mention specifics in the interest of protecting information.

Six noted that the level of information or guidance provided would depend on the nature and extent of any breach and the data involved.

Two noted that it would up to clients to decide what information to provide.

A handful (three each) also noted other information they would provide including the following.

- Providing regular updates to parties involved and how it is being dealt with.
- Advising users to change their passwords.
- Assurance that a similar event would not occur again.

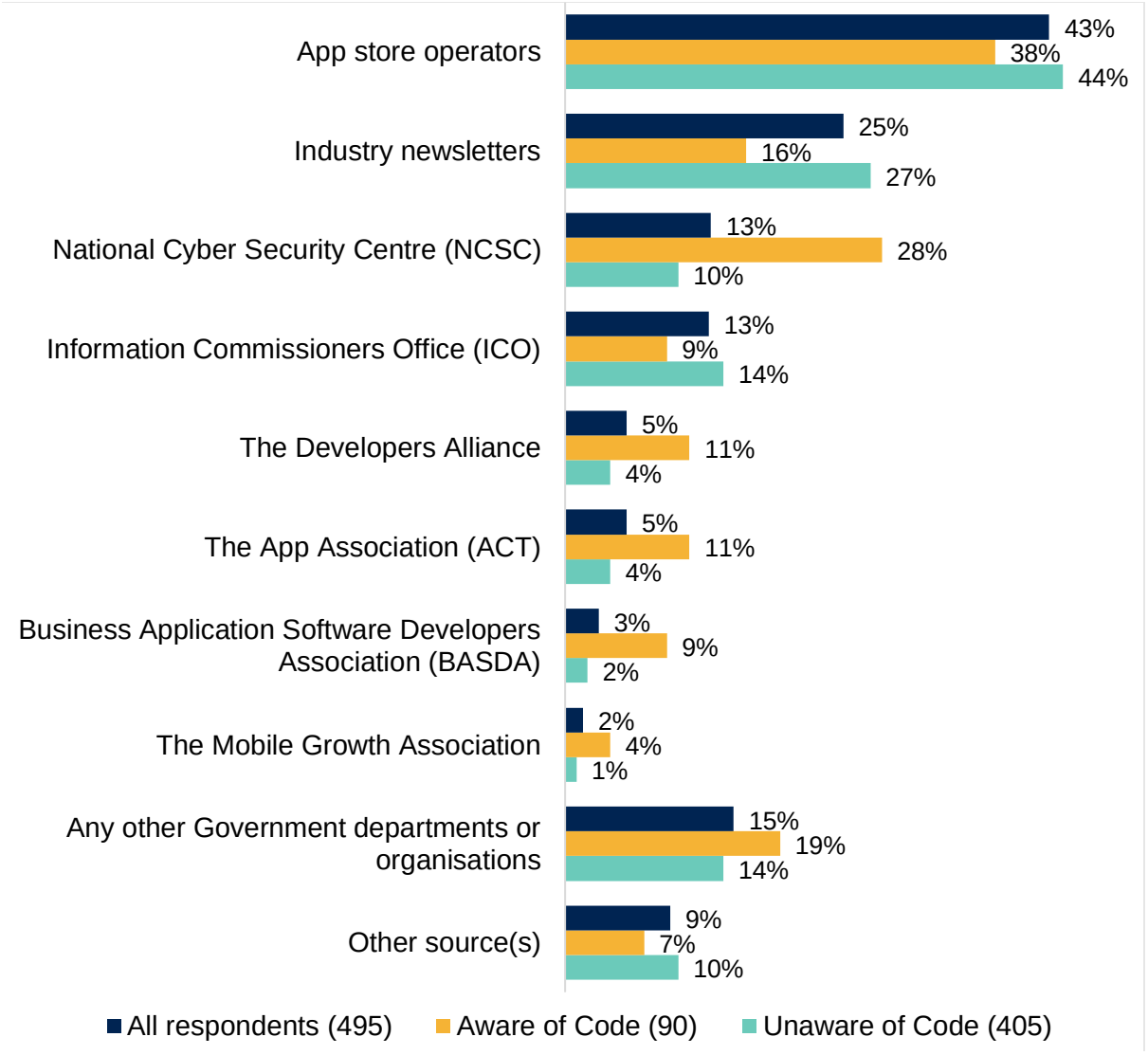
# 4. Keeping up to date on security and privacy practices

This chapter discusses what sources app developers access to keep up to date on security and privacy matters, and their perceived utility. The nature and extent of engagement with app store operators is also explored.

## 4.1 Sources accessed and their utility

Specifically in relation to matters focusing on app development security and privacy, the most commonly accessed or used source of information by surveyed app developers over the last 12 months is that from app store operators (43%) and industry newsletters (25%).

**Figure 22 Sources used to stay up to date on app development security and privacy**




(Multiple responses permitted.) Source: Pye Tait Consulting 2023.

'Other' sources were mentioned by 46 respondents. Commonly mentioned sources include the following.

- Microsoft guidelines (four)
- Cyber Essentials (four)
- NHS standards (four)
- GDPR (four)
- Networking with peers and colleagues (four)
- ISO (three)
- A range of other sources each mentioned by one respondent.

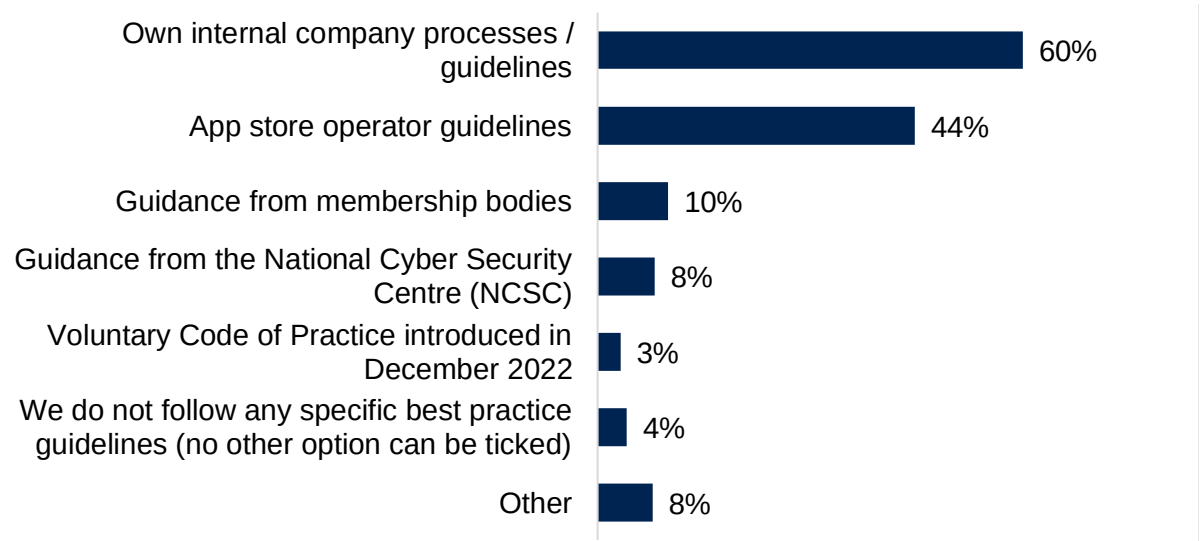
Surveyed app developers aware of the Code of Practice are significantly more likely to have accessed or used information from NCSC (28% vs 10%), The App Association (11% vs 4%), The Developers Alliance (11% vs 4%), BASDA (9% vs 2%) and The Mobile Growth Association (4% vs 1%). In contrast, those unaware of the Code are significantly more likely to have accessed or used information in industry newsletters compared to those unaware of the Code (27% vs 16%). Taken together, this would indicate that app developers who are more likely to have heard of the Code are those who ensure they keep up to date on latest sector developments through different avenues.

Meanwhile, surveyed app developers based overseas are – compared to most UK regions/nations – significantly more likely to keep up to date via The Developers Association.

### 4.1.1 Standards, legislation, and guidelines followed

Asked what standards and best practice guidelines they currently use in their app development process, three in five (60%) surveyed app developers follow their own internal company processes when developing apps. Over two in five (44%) follow guidelines from app store operators.

**Figure 23 Standards and guidelines currently used in app development process**




Base: 587 respondents (multiple responses permitted). Source: Pye Tait Consulting 2023.

'Other' guidelines or standards were mentioned by 45 respondents, with common mentions including the following.

- ISO (nine)
- O Wasp guidelines (four)
- Microsoft (three)
- Client requirements (three)
- Penetration testing (three)
- Government sources (two)
- ICO (two)
- NHS (two)
- A range of different guidance each mentioned by one respondent.

Surveyed app developers aware of the Code of Practice are significantly more likely – compared to those unaware of the Code – to currently use guidance from NCSC (18% vs 6%) or the Code itself (12% vs 2%). In contrast, those unaware of the Code are significantly more likely to follow their own internal processes than those aware of the Code (64% vs 38%).

Meanwhile, those developing apps for laptops/desktops are significantly less likely to currently use app store operator guidelines compared to those developing apps for other platforms.

Surveyed app developers based overseas were significantly less likely – compared to most UK regions – to have their own internal processes (noted by 23% of such) and were significantly more likely to say they do not follow any specific best practice guidelines (18%).

Further to this, interviewed app developers were asked what legislation and/or guidance their organisation uses to guide the development of their apps for the UK market.

Just under half (nine) said GDPR is a key source guiding their app development, being a legislative core of developmental procedures, especially when dealing with personal data.

Six said there was no one overarching source guiding their app development, but instead use multiple different digital landscapes and infrastructures during development, noting how guidance can vary between these. Three say they have internal organisational guidelines they follow, and with some noting the need for apps to be accessible.

Client-specific guidelines also play a role in app development. However, five interviewees noted there are broad similarities in the guiding and legislative expectations of clients.

### 4.1.2 Usefulness of information sources

In terms of the usefulness of information relating to app security and privacy from different sources, NCSC and app store operators were rated most highly (both average 8.4) – on a scale from one (not at all useful) to 10 (extremely useful). Scores provided for each source are relatively high, with no source averaging below 7.7.

**Table 6 Usefulness of information provided by different sources**

| Source (base) | Average |
|---|---|
| NCSC (62) | 8.4 |
| App store operators (205) | 8.4 |
| The Mobile Growth Association (7) | 8.1 |
| Other government departments or organisations (72) | 8.1 |
| Industry newsletters (121) | 8.0 |
| The Developers Alliance (27) | 7.9 |
| The App Association (ACT) (25) | 7.9 |
| BASDA (14) | 7.7 |
| ICO (63) | 7.7 |
| Other source(s) (41) | 9.0 |

Source: Pye Tait Consulting 2023.

Those who scored a six or below for any source were asked to explain their response, to outline why the information provided is not felt to be able useful as it might be, and 33 responses were received. Around half of these (15, 45%) asserted that information given is, in some way, poor – for example some (seven, 21%) said information was not wholly relevant, lacked specific details (three, 11%), or was not extensive enough (three, 11%).

Some (nine, 27%) stated that it was difficult to get in contact with the organisation in question – this was particularly noted in relation to app store operators – indeed some interviewed app developers identified long response times as an issue regarding app discussion, with one claiming they often wait for days to be granted the ability to implement an update.

A couple (two, 6%) found it difficult to locate relevant information within sources.

Interviewed app developers were also asked how helpful guidance and/or legislation is for their app development.

Four think the guidance and/or legislation they follow is crucial for their app development, noting that the reworking of GDPR in recent years to be made clearer is appreciated. They also pointed out that legislation, by its nature, must be conformed to, to operate in the market, but that aligning to regulations is important to secure commercial opportunities, as well as acting to protect the company's reputation and integrity.

Five described the guidance and/or legislation they follow as very helpful for their app development, saying this aids staff in understanding required levels of security and privacy during app development, fostering a safer environment for organisations and clients.

Three mentioned that they are flexible to client requirements but would not necessarily call such guidance helpful.

### 4.1.3 Additional guidance

In terms of other guidance that might be helpful for their organisation when developing apps for the UK market, six interviewees suggested that some form of online resource would be useful – a staged checklist for app developers is commonly mentioned in this regard, with suggestion this could contain elements of privacy, security and accessibility.

Four stated that a central point of information from government would be helpful for organisations when developing apps, to act as a one-stop shop.

A desire to see further guidance on international requirements when developing apps is asserted by four interviewees. It was stressed that app development is a global market. One proposed a source detailing dos-and-do-nots with UK app development so that international countries can become more acquainted with UK app privacy and security. Another participant with clients from various countries thinks that this would be useful as a means of comparing requirements between countries.

Three suggested that additional guidance from app store operators would be helpful for organisations when developing apps. One noted that app store operators are not always forthcoming with their guidance.

> *It doesn't need to be anything sophisticated – just an online resource with checklists an organisation can go through. A combined resource – security, privacy and accessibility. – Small size firm, Scotland, Unaware of Code*

## 4.2 Engagement with app store operators

### 4.2.1 General engagement

Twelve interviewed app developers stated they do not have a dedicated, named point of contact across any app store, with only one claiming to have a direct point of contact. Engagement with app store operators instead tends to be on a more ad hoc basis, and only when necessary, for instance when an app is rejected or accepted. In such cases developers are often notified as to the reasons for this, and the problems they must fix to get an app on the market.

Four asserted that communication can vary between app stores operators. Two pointed out how Apple are meticulous when reviewing and testing functionality, and have stricter guidelines concerning app privacy and security, therefore rejection of prospective apps is more commonplace.

Three interviewees noted they receive regular updates from app store operators pertaining to privacy and security, although in contrast four noted they do not receive regular updates on these matters. It was suggested this differential may arise where apps have more users or are more visible or successful and app store operators are in closer contact with developers. Three believe that communication with app store operators is dependent on the size and success of the business, with more regular or personalised communication more likely for those with a larger install-base.

One claimed they had received recognition from operators pertaining to metrics like security standards and user ratings, which has led to regular, ongoing communication.

Two developers said they work as part of an agency meaning their respective clients will deal directly with app store operators, and so will not have direct communication.

Four interviewees claimed that security guidelines and checks from app store operators have become more stringent in recent years.

> *At one stage, you could publish an app and it would be live in a couple of hours. The last four or five years they've added more structure, being a little bit more thorough, making sure people do have things like privacy policies and statements. – Small size firm, East Midlands, Unaware of Code*

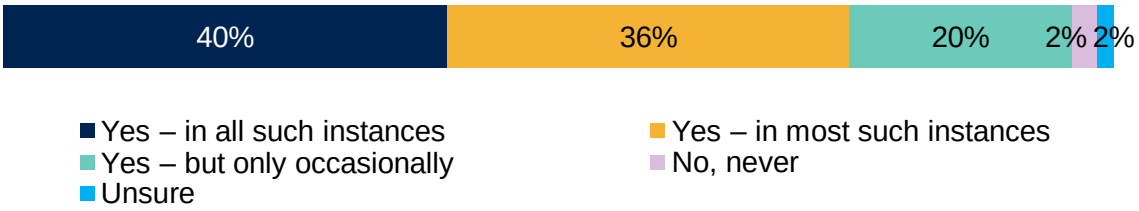
### 4.2.2 Instances where apps are rejected by app store operators

The Code of Practice was developed to set out practical steps for app store operators and app developers to protect users. Principle 1 of the Code is to ensure only apps that meet the Code's security and privacy baseline requirements are allowed on the app store.

The average (mean) proportion of apps which surveyed app developers say app store operators have initially rejected on security and privacy grounds is 5%. Just under three quarters (74%) say they have never had an app rejected on this basis.

Those surveyed app developers who had had an app rejected in such instances were asked if app store operators had provided actionable feedback to be compliant with security and privacy requirements. Two in five (40%) said this was provided in all such instances, and a slightly smaller proportion (36%) said in most instances.

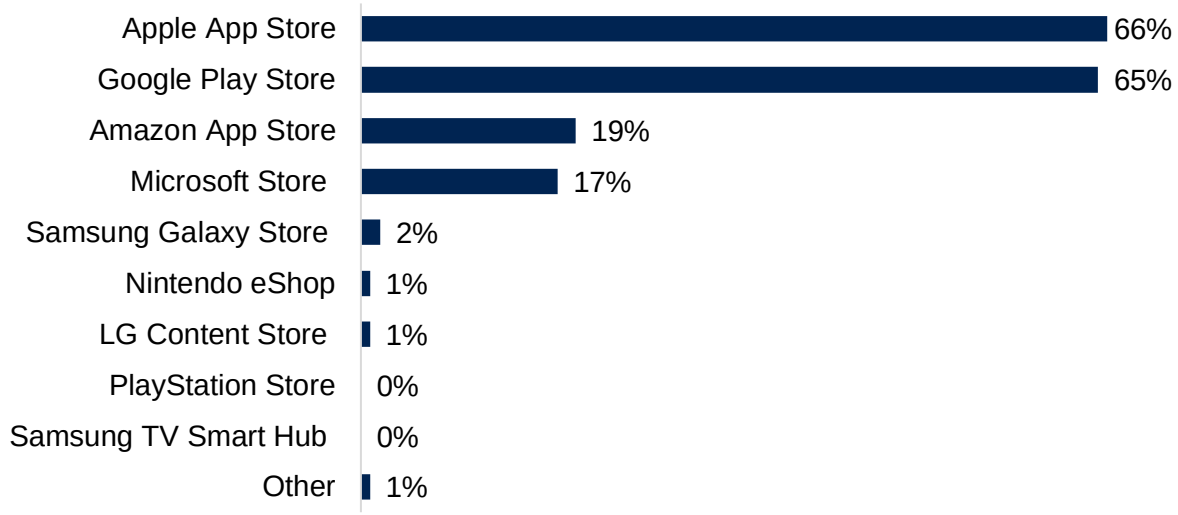
**Figure 24 Whether app store operators provided actionable feedback**




Base: 130 respondents (those who had had an app rejected on security or privacy grounds).
Source: Pye Tait Consulting 2023.

Those surveyed app developers who had had at least one app rejected on security and privacy grounds, were presented with a list of app store operators for which they had previously said they develop apps for, and asked which app store operators had rejected any of their submissions. The most common app store operators to do so are Apple App Store (66%) and Google Play Store (65%), followed by Amazon App Store (19%) and Microsoft Store (17%). The one 'other' response mentioned was Salesforce.

**Figure 25 Stores rejecting app submissions on security and privacy grounds**




Base: 121 respondents (those who had had an app rejected on security or privacy grounds). (Multiple responses permitted.) Source: Pye Tait Consulting 2023.

There were no substantial differences of note by app developers' size, awareness of the Code, or platform.

Interviewed app developers noted that, if an app is rejected, operators tend to offer advice on how to resolve certain issues, however, many said there is limited or no formal correspondence.

> *There is no formal discussion, you basically send something out and you get told if it's been rejected or accepted, and if it is rejected, they give you the why, but that's about it. – Micro size firm, South East, Unaware of Code*

# 5. Conclusions

The chapter reflects on the evidence gathered through this research to pull together the key findings, linking back to the research objectives.

### Objective 1: Assess app developers' awareness of the Code of Practice, their views on barriers to uptake of the Code, and what has driven some developers to take up the Code.

Around one in six (16%) app developers are aware of the Code of Practice that was published in December 2022. Of those who are aware, the Code has been positively received on the whole, with the Code helping to establish more robust security and privacy processes and being straightforward to integrate within existing internal processes. Indeed, a sizeable proportion see no barriers to implementing the Code's principles, other than on staff time. Alignment to the Code has in turn also helped strengthen opportunities for commercial success by demonstrating adherence to government guidelines to potential clients.

Among those who are unaware, there is generally a good appetite for the idea of a set of voluntary guidelines.

Improvements put forward include the Code being rather long and text-heavy, and hard to digest.

App developers suggest that substantial engagement and promotion is required to raise awareness of the Code among the app developer community.

### Objective 2: Understand whether security and privacy practices that app developers currently have in place have been influenced by the Code of Practice (Principles 2, 3, 4).

There are varying views among app developers as to the extent to which the Code has fundamentally influenced their security and privacy practices, however, feedback on the Code is generally positive that it will help to protect consumers.

There are varying degrees of alignment to each of the Code's principles, although this depends to a large extent on app developers' circumstances and whether all principles are necessarily applicable (for instance if their apps do not process or store personal data, or are bespoke and not available via app stores).

However, of note is that a significantly lower proportion of those unaware of the Code do have plans to implement certain practices that align to the Code's principles.

**Objective 3: Understand how app developers provide security and privacy information to users in an accessible way (Principle 5).**

There is good alignment with the Code's principles on this, with 82% sharing information on when the app was last updated and 74% signposting to where users' data is stored, for all apps they develop. Other information is also provided to users in some situations and this can include additional security information, extra security protocols and encryption.

**Objective 4: Understand what steps or processes are in place by app developers if they become aware of a security incident or a personal data breach (Principle 8).**

App developers' current practices are in reasonable alignment to the Code's principles in this regard (between 62% and 84% of app developers' activities align, for all apps they develop). However, some practices are not applicable for certain developers for all their apps, and the extent of information and detail that would be provided to users and other parties varies between app developers.

Again, a significantly lower proportion of those unaware of the Code have plans to implement certain practices that align to the Code's principles.

**Objective 5: Understand whether app store operators are signposting the Code of Practice (and other relevant guidance) to developers prior to an app's submission (Principle 6).**

and

**Objective 6: Understand the prevalence of rejected apps under the Code of Practice and whether app developers have received actionable feedback from app store operators to make the app compliant with the Code of Practice (Principle 7).**

Key findings can be grouped together to answer these two research objectives.

Of those who could recall at what point an app store operator provided signposting to the Code, the majority said that this was prior to app submission, with a minority saying it only happened post-submission.

Around 5% of apps are rejected on the basis of security and privacy concerns. Actionable feedback is generally provided although around one fifth note this only happens occasionally or not at all.

More generally, few app developers have a dedicated point of contact with app store operators, and engagement tends to be more on a more ad hoc basis, as and when issues arise.

**Objective 7: Understand where/if app developers get support (i.e. members of bodies etc.).**

The information source most commonly used or accessed by app developers is app store operators, while industry newsletters and NCSC are also referred to frequently. Closer working relationships between developers and operators mean that substantial weight is

placed on app store operator guidelines, sometimes above the Code, with operators ultimately being the 'gatekeeper' to an app's publication.

In terms of legislation and guidance, GDPR plays a key role in steering app development.

Generally, app developers receive information and support from a variety of different sources.

### Objective 8: Understand the costs involved with implementing the requirements of the Code and whether, if fully complying with the Code of Practice, these would cause any business to drop out of the market.

It was difficult for many app developers to provide figures in relation to the costs involved in implementing the Code's requirements.

Of those that could provide a top-level estimate, costs were wide-ranging (skewed by few large estimates) but taking the median costs as a benchmark would appear to indicate that any financial burden would be between £400 to £800 (although it is unclear whether these are short-term or ongoing costs, or whether this scales by business size).

A large minority (36% of those aware of the Code, and 43% of those unaware of the Code) feel such costs will not impact their business at all, usually because they already comply to the Code's requirements. Any costs would be most likely related to staff time or to implement new procedures.

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:

Certificate Number 10745