香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

1996-2021
守護 · 私隱 · 廿五載
GUARDIAN · PRIVACY · 25 YEARS

Survey of Data User Attitudes on Personal Data Privacy Protection 2020

Report

28 January 2021

THE UNIVERSITY OF HONG KONG
SOCIAL SCIENCES RESEARCH CENTRE
Director: Professor J. Bacon-Shone *(PhD Birmingham)*

香港大學
社會科學研究中心
主任: 白景崇教授

Table of Contents

Preface

Personal data privacy is of mounting importance nowadays as public expectation on the protection of privacy escalates in an age of rapid technological developments and extensive use of social media. As the authority entrusted to monitor and supervise the compliance with the provisions of the Personal Data (Privacy) Ordinance, Cap. 486 ("PDPO") and promote awareness and understanding of the requirements of PDPO, it is incumbent on my Office (the "PCPD") to gauge the awareness and views of the public and organisations on the protection of personal data privacy from time to time. To this end, the PCPD commissioned the Social Sciences Research Centre of The University of Hong Kong ("HKUSSRC") to conduct a survey in the period between May and October 2020. The survey comprised two parts, one targeting individual members of the public (i.e. data subjects), and the other targeting organisations (i.e. data users).

The objectives of the survey were to understand, among others, (i) the public's knowledge of and sensitivity towards the protection of personal data privacy; (ii) the difficulties of organisations in complying with the PDPO; (iii) the effectiveness and expectation of the work of the PCPD; and (iv) the level of support on possible directions of amendments to the PDPO.

I would like to express my gratitude to HKUSSRC and its Director, Professor John Bacon-Shone, for the successful conduct and completion of the survey in a highly professional manner. I would also like to offer my personal thanks to all respondents of the survey for their valuable contributions.

The results of the survey will certainly serve as a good reference for the PCPD in making informed decisions on regulatory strategies and the contents of our educational or promotional activities in future. I hope that all stakeholders will also find the survey results useful in enhancing their awareness, and the protection, of personal data privacy.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data, Hong Kong

January 2021

Executive Summary

Methodology

1. A total of 227 responses were obtained, 203 via a telephone survey and 24 via an online survey. Although the low response rate meant the survey cannot be projected to the entire population of data users in Hong Kong, it represents the views of a wide-ranging set of data users in terms of both industry sectors and number of Hong Kong employees, and should have considerable value in elaborating the views of data users on data protection and privacy.

Summary of the Data User Survey

Demographic profile of respondents

2. The combined sample is broadly representative, as it consists of responses from 13 different sectors. The sample has not been weighted to match the data of the Census and Statistics Department, as the low response rate makes it questionable whether we have a statistically representative result. However, the wide range of sectors included allow us to see the range of views across different sectors. Although small establishments (1-9 employees in Hong Kong) are the most common in our sample, we have representation across all sizes of establishments.

Privacy Management Programme ("PMP")

3. For the level of understanding of PMP, the most common answer was no understanding at all (a rating of 0 on a scale from 0 to 10), by 25% of respondents, however 37.9% rated their level as 6 or above. For the stage of implementation of PMP, the most common stage is no implementation at all (a rating of 0), by 27.3%, however 49.7% reported the stage as 6 or above. The primary benefit of PMP most commonly reported (70 responses) was better data protection, followed by better compliance (5 responses), with all other responses only occurring once or twice. The primary difficulty in implementation of PMP most commonly reported was difficulty in educating employees (7 responses), followed by lack of management support (4 responses) and lack of clarity in PMP (3 responses).

Data Protection Officer ("DPO")

4. Only 17.6% of respondents have a DPO.

Privacy Impact Assessment ("PIA")

5. Only 14.1% of respondents have undertaken a PIA.

Compliance and complaints

6. For the difficulty that respondents have with compliance with the Personal Data (Privacy) Ordinance ("PDPO"), the most common answer is 5 (on a scale from 0 to 10), by 21.4% of respondents, with 21.4% reporting the difficulty as 6 to 10. For the number of privacy-related complaints that respondents have had received in the last 12 months, the overwhelming majority (94.6%) reporting no complaints, with a mean number of complaints of about 40 per organization, suggesting that most of the complaints relate to a small number of data users.

Knowledge of relevant Mainland China laws and regulations

7. Most respondents do not have good knowledge of the two major Mainland China laws and regulations on personal data protection, with more than half reporting no knowledge (0 on a scale from 0 to 10) of the Cybersecurity Law (58.9%) and the Personal Information Security Specification (59.0%).

Awareness of the Office of the Privacy Commissioner for Personal Data ("PCPD")

8. Awareness of the PCPD publicity materials through mass media, advertisements (other than mass media), publications, website/social media and events is highest for mass media (59%), followed by advertisements (other than mass media) (28%), website/social media (25%), publications (24%) and events (12%). For the most helpful form of additional support from the PCPD, the most common suggestion was better promotion/publicity, especially online (27 responses); followed by free or online training (13 responses) and better distribution of materials (10 responses).

Support for possible amendments to the PDPO

9. The data user survey covered seven major possible amendments to the PDPO. For significant data breaches (such as the Cathay Pacific case), the amendments considered were (1) requiring organisations to notify the PCPD, (2) giving the PCPD the power to require customers to be notified and (3) including financial penalties in the PDPO. For significant misuse of personal data (such as doxxing), amendments considered were (4) requiring removal of contents from social media platforms and websites that are controlled by entities in Hong Kong, (5) requiring removal of contents from social media platforms and websites that are controlled by entities overseas, (6) giving the PCPD the power of criminal investigation and (7) giving the PCPD the power of prosecution for cases like this. The support for these seven amendments is quite high, with over 80% supporting at a rating

of 6 and above (on a scale from 0 to 10) for the three data breach related amendments (over 60% giving full support for the notification amendments and over 45% giving full support for the penalties amendment) and over 60% supporting at a rating of 6 and above for the four doxxing related amendments (around 30% giving full support for all four amendments).

10. The online survey covered another eleven possible amendments to the PDPO, covering (1) specification of the data retention period, (2) regulation of data processors, (3) clarifying the definition of personal data, (4) adding a legal requirement on privacy accountability, (5) enhancing regulation of sensitive personal data, (6) providing stronger protection for the personal data of children, (7) updating the regulation of cross-boundary/border transfer of personal data, (8) adding the right to be forgotten, (9) adding the right to object to automated decision-making, (10) adding the right to data portability and (11) repealing the data user return scheme. As the online survey was mainly completed by members of the Data Protection Officers' Club of the PCPD, we would expect that these respondents should be relatively well aware of the rationale for these amendments. From the online survey, the level of support for all eleven possible amendments to the PDPO was at least 70% supported at a rating of 6 and above (on a scale from 0 to 10). Clarification of what is personal data, enhanced protections for sensitive personal data and children's personal data had full support from at least 40%. Regulation of data processors, privacy accountability, updating the cross-boundary/border protections, the right to be forgotten, rights regarding automated decisions and repealing the data user return scheme had full support from at least 30%. Retention policy and portability rights had full support from at least 20% of online survey respondents.

Implementation stage and privacy risks of new technologies

11. From the online survey, we have information about the stage of implementation of Artificial Intelligence (AI), Big Data, Blockchain, Cloud Computing and Internet of Things (IoT) and about their perceived privacy risk as regards excessive collection of personal data, transparency, change of use, security and unnecessary retention of personal data. For the stage of implementation, Cloud Computing (50% implemented) and IoT (41.7% implemented) are furthest ahead. Again, as the online survey was mainly completed by members of the Data Protection Officers' Club, we would expect that these respondents should be relatively well aware of the privacy risks of these new technologies. The respondents reported that AI and Big Data are generally seen to involve high privacy risk, specifically as regards excessive collection of personal data (64.3% for AI, 62.5% for Big Data), transparency in personal data processing (57.1% for AI, 50.0% for Big Data), change of use of personal data (57.1% for AI, 50.0% for Big Data), unnecessary retention of

personal data (47.1% for AI, 43.8% for Big Data) and data security (50.0% for AI, 43.8% for Big Data).

Recommendations

Privacy Management Programme

12. While more than a third of the respondents reported their level of understanding of PMP as 6 or above, around a quarter had no knowledge at all, suggesting a broader need for educating organizations about the concepts of PMP, so that they at least understand its relevance. The stage of implementation matches up, with about a quarter having no implementation at all. However, it is clear that most respondents clearly understood that the primary benefit of PMP is better data protection. The primary difficulty in implementing PMP most commonly reported was difficulty in educating employees, again highlighting the need for additional training.

Data Protection Officer and Privacy Impact Assessment

13. Less than 20% of respondents have a DPO or undertaken a PIA, suggesting a need to persuade organizations of the value of a DPO and the PIA process.

Compliance and complaints

14. The level of difficulty in compliance with the PDPO reported is very variable, indicating the need for identifying the sectors with greater difficulty in compliance (the PCPD data on complaints is probably a sound basis for this). As the overwhelming majority reported no privacy-related complaints, this suggests that most of the complaints relate to a small number of data users and hence the continuing need for a targeted approach.

Knowledge of Mainland China laws and regulations on data protection

15. The majority of respondents reported no knowledge of the two major Mainland China laws and regulations on data protection, though the survey does not allow us to check whether that knowledge is relevant, so targeted training may arguably be required.

Awareness of the PCPD

16. Awareness of the PCPD publicity materials through mass media, advertisements (other than mass media), publications, website/social media and events is highest for mass media, followed by advertisements (other than mass media), website/social media, publications and events, suggesting the need for some consideration of updating the publicity strategy, especially given that the most common request for additional support from the PCPD was

better promotion/publicity, especially online; followed by free or online training and better distribution of materials.

Support for possible amendments to the PDPO

17. The level of support for the seven possible amendments to the PDPO relating to significant data breaches and significant misuse of personal data (such as doxxing) was high, especially for notification of the PCPD and customers and financial penalties for significant data breaches, such as the Cathay Pacific case, although the level of support is less for the four doxxing related amendments.

18. The online survey covered another eleven possible amendments to the PDPO. As the online survey was mainly completed by members of the Data Protection Officers' Club, it is important to be cautious in interpreting the high level of support for these eleven possible amendments. However, clarification of what is personal data, enhanced protections for sensitive personal data and personal data of children had the highest level of full support, suggesting that they could be prioritized in that informed data users are more likely to support these amendments. Regulation of data processors, privacy accountability, updating the cross-boundary/border protections, the right to be forgotten, rights regarding automated decisions and repealing the data user return scheme has a lower level of support. Retention policy and portability right had the weakest level of full support.

Implementation stage and privacy risks of new technologies

19. From the online survey, we see that Cloud Computing and IoT are furthest ahead in implementation. However, AI and Big Data are generally seen to involve high privacy risk by about half of respondents, as regards excessive collection of personal data, transparency in personal data processing, change of use of personal data, unnecessary retention of personal data and data security, suggesting that the high privacy risks might be one reason why these technologies are behind in implementation and hence suggesting that the PCPD guidance is most important in these domains.

Chapter 1 Introduction

1.1 Background

The Office of the Privacy Commissioner for Personal Data ("PCPD") is an independent body established to monitor, supervise and promote compliance with the Personal Data (Privacy) Ordinance ("PDPO"), which was enacted to protect the personal data privacy rights of individuals and to provide for the regulation of the collection, holding, processing, security and use of personal data. The PCPD commissioned the Social Sciences Research Centre of The University of Hong Kong ("HKUSSRC") to conduct a survey of the attitudes of data users (i.e. establishments that collect or use personal data) on personal data privacy protection, so as to provide the PCPD with a useful reference to make informed decisions on strategies and educational/promotional activities in the future.

1.2 Research Objectives

The objectives of the Study were to understand the following:

1. Implementation of privacy accountability by data users;
2. Difficulties encountered by data users in complying with the requirements of the PDPO;
3. Forms of support expected of the PCPD for data users' compliance with the PDPO;
4. Data users' views on the possible amendments to the PDPO; and
5. Adoption rate of new ICT, such as AI, Big Data, Blockchain, Cloud Computing and IoT, in collecting and processing personal data by data users.

1.3 Organisation of the Report

The report is divided into three chapters: Chapter 1 contains the background and research objectives, Chapter 2 covers the survey results in detail and Chapter 3 provides a summary of the findings.

Chapter 2 Survey Results

2.1 Survey Research Methodology

2.1.1 Study Design and Target Respondents

The Study was conducted through a telephone survey and an online survey. The target population of the telephone survey is all Hong Kong establishments, so a sample was drawn from the Census and Statistics Department Central Register of Establishments, linked to the White Pages to obtain telephone numbers. The telephone survey contains only the core questions from the survey questionnaire, in order to keep the completion time to a reasonable limit. For the online survey, the PCPD sent links to 10 chambers of commerce and the 364 members of the PCPD's Data Protection Officers' Club. The assumption was that this target would be more knowledgeable about the PDPO and hence willing to complete a longer online questionnaire.

2.1.2 Ethical Approval

Ethical approval was obtained from the Human Research Ethics Committee for Non-Clinical Faculties of The University of Hong Kong prior to the commencement of the Study.

2.1.3 Pilot Studies

A pilot study of the telephone survey comprising 9 successfully completed interviews was conducted between 26 June and 29 June 2020. Three interviewers participated in the pilot survey in the form of telephone interviews using a Computer Aided Telephone Interview ("CATI") system, calling from 4:30pm to 10:30pm. All interviewers studied the questionnaire instructions and completed a practice interview before making phone calls. The supervisor reviewed the interviews to see whether they were employing proper question-asking and probing techniques and conducting the interview in a professional manner. General problems were noted and instructions were clarified for every interviewer.

A pilot study of the online survey comprising three complete submissions was conducted between 24 August and 8 September 2020. The three participants were contacted to obtain feedback on any problems with the questionnaire.

Based on the feedback and comments from participants and the PCPD, the questionnaires and the logistics were fine-tuned. Data collected from the pilot telephone interviews are not included in the analysis reported below.

2.1.4 Data Collection

A total of 203 telephone interviews were successfully completed between 6 August and 3 September 2020 via a telephone survey of randomly selected businesses using the CATI system, calling between 2:00pm and 6:00pm. All interviewers studied the questionnaire instructions and successfully completed a practice interview before making phone calls. The supervisor reviewed the interviews to see whether the interviewers were employing proper question-asking and probing techniques and conducting the interviews in a professional manner. General problems were also noted and instructions were clarified for every interviewer.

A total of 24 online survey responses were received between 1 September and 20 October 2020.

2.1.5 Quality Control

The following quality control measures were incorporated in the Study:

- The data collected was subjected to range checking and logical checking. Unclear and illogical answers were re-coded as invalid.
- Questionnaires with more than half of the questions unanswered were regarded as incomplete questionnaires and excluded from analysis.
- Any missing answers were excluded from analysis.
- Quality checking procedures were applied to at least 10% of the data collected prior to analysis and use, to ensure that the data was valid.

2.1.6 Response Rate

A total of 2,211 telephone numbers were attempted for the telephone survey component. However, 866 were not available at that time, 250 refused, 839 did not answer and 53 were invalid. Ultimately, a total of 203 respondents were successfully interviewed by using the CATI in the survey. The overall contact rate was 60.0%[1] and response rate was 44.8%[2]. Table 1 shows the detailed breakdown of final telephone contact status.

We also obtained 24 online responses, of which 23 were from the 364 members of the PCPD's Data Protection Officers' Club (response rate of 6.3%) and 1 was from a member of a chamber of commerce.

[1] Contact rate = the number of answered telephone calls divided by the total number of calls attempted, i.e. sum of (Types 1 to 6) / Total = (203+0+250+8+0+866)/2,211 = 60.0%.

[2] Response rate = the number of successful interviews divided by the sum of the numbers of successful interviews, partial cases and refusal cases, i.e. (Type 1) / (Type 1 + Type 2 + Type 3) = 203/(203+0+250)=44.8%.

Table 1: Final status of telephone numbers attempted

Type	Final status of contacts	Number of cases
1	Success	203
2	Partial	0
3	Refusal	250
4	No such company or closed	8
5	Language problem	0
6	Not Available	866
7	No Answer	839
8	Fax	10
9	Invalid	35
	Total	2,211

2.1.7 Overall Sampling Error

The telephone survey findings are subject to sampling error. For a sample size of 203, the maximum sampling error is + 6.9% at the 95% level of confidence (ignoring clustering effects). In other words, we have 95% confidence that the population proportion falls within the sample proportion plus or minus 6.9%, based on the assumption that non-respondents are similar to respondents. The response rate for the online survey was low, making the assumption of a representative sample less reasonable.

2.1.8 Quality Control

All SSRC interviewers were well trained in a standardised approach prior to the commencement of the survey. All interviews were conducted by experienced interviewers fluent in Cantonese, Putonghua and English.

The SSRC engaged in quality assurance for each stage of the survey to ensure satisfactory standards of performance. At least 5% of the questionnaires completed by each interviewer were checked by the SSRC supervisors independently.

2.1.9 Data Processing and Analysis

Descriptive Statistics

Descriptive statistics are used to summarise the findings of the Study and they are reported in frequency, percentages, means and standard deviations (SD), wherever appropriate. Some percentages might not add up to the total or 100% because of rounding. Moreover, the sample

bases for each question might vary due to missing answers, as those who refused to answer or who stated that they did not know are excluded from the tables. All statistical analysis used the software JMP version 14.3.

2.1.10 Final Questionnaire

The final questionnaire for the data user survey can be found in Appendix A. It covers all the research objectives. The questionnaire indicates which questions were only included in the online survey.

2.2 Findings from the Survey

2.2.1 Demographic profile of respondents

Table 2 shows that the combined sample is broadly representative, in the sense that we have responses from 13 different sectors. The sample has not been weighted to match the data of the Census and Statistics Department, as the low response rate makes it questionable whether we have a statistically representative result, but the wide range of sectors included means that we should be able to see the range of views across different sectors.

Table 2: Industry Sector	Count	%
Retail	32	14.1%
Social/Personal	28	12.3%
IT/Communications	26	11.5%
Finance/Insurance	26	11.5%
Accommodation/Food	24	10.6%
Professional/Business services	21	9.3%
Import/Export/Wholesale	18	7.9%
Transport/Storage/Logistics	17	7.5%
Manufacturing	14	6.2%
Construction	9	4.0%
Electricity/Gas supply/Waste management	7	3.1%
Real estate	3	1.3%
Travel	2	0.9%
Total	227	100.0%

Table 3 shows that although small establishments (having 1-9 employees in Hong Kong) are the most common in our sample, we have representation across all sizes of establishments.

Table 3: No. of Employees in Hong Kong	Count	%
1-9	123	54.2%
10-19	49	21.6%
20-49	21	9.3%
50-100	11	4.8%
100+	23	10.1%
Total	227	100.0%

We next examine the questions included in both the telephone and online surveys.

2.2.2 Privacy Management Programme ("PMP")

There were four questions about PMP covering level of understanding (on a scale from 0 to 10), primary benefit, primary difficulty and stage of implementation (on a scale from 0 to 10).

Table 4 shows the level of understanding of PMP, which shows that the most common answer was no understanding at all (0), by 25% of respondents. However, 37.9% rated their level as 6 or above.

Table 4: Level of understanding of PMP (0-10)	Count	%
0	56	25.0%
1	3	1.3%
2	10	4.5%
3	14	6.3%
4	12	5.4%
5	44	19.6%
6	27	12.1%
7	22	9.8%
8	22	9.8%
9	5	2.2%
10	9	4.0%
Total	224	100.0%

Table 5 shows the stage of implementation of PMP, where the most common stage is no implementation at all (0), by 27.3%. However, 49.7% reported the stage as 6 or above.

Table 5: Stage of PMP implementation	Count	%
0	44	27.3%
1	2	1.2%
2	2	1.2%
3	4	2.5%
4	5	3.1%
5	24	14.9%
6	16	9.9%
7	28	17.4%
8	13	8.1%
9	7	4.3%
10	16	9.9%
	161	100.0%

The respondents were asked about the primary benefit and difficulty of PMP by open-ended questions. The primary benefit most commonly reported (70 responses) was better data protection, followed by better compliance (5 responses), with all other responses only occurring once or twice. The primary difficulty most commonly reported was difficulty in educating employees (7 responses), followed by lack of management support (4 responses) and lack of clarity about PMP (3 responses).

2.2.3 Data Protection Officer ("DPO")

Table 6 shows that only 17.6% of respondents have a DPO.

Table 6: Have a DPO?	Count	%
Yes	40	17.6%
No	184	81.1%
Don't Know	3	1.3%
Total	227	100.0%

2.2.4 Privacy Impact Assessment ("PIA")

Table 7 shows that only 14.1% of respondents have undertaken a PIA.

Table 7: Undertaken a PIA?	Count	%
Yes	32	14.1%
No	181	79.7%
Don't Know	14	6.2%
Total	227	100.0%

2.2.5 Compliance and complaints

Table 8 shows the level of difficulty that respondents have with compliance with the PDPO, on a scale from 0 to 10, where 0 means no difficulty at all and 10 means very difficult, where the most common answer is 5, by 21.4% of respondents. Meanwhile, 57.1% of respondents gave answers between 0 and 4 and the remaining 21.4% reported answers between 6 and 10, suggesting wide variability in the level of difficulty.[3]

Table 8: Level of difficulty in compliance with PDPO (0-10)	Count	%
0	39	18.6%
1	12	5.7%
2	23	11.0%
3	31	14.8%
4	15	7.1%
5	45	21.4%
6	9	4.3%
7	18	8.6%
8	9	4.3%
9	0	0.0%
10	9	4.3%
Total	210	100.0%

[3] Analysis of level of difficulty in compliance with the PDPO by number of employees and industry sector did not show any clear pattern as neither variable explained much of the variability in level of difficulty.

Table 9 shows the number of privacy-related complaints that respondents have had received in the last 12 months, with the overwhelming majority (94.6%) reporting no complaints and a mean number of complaints of about 40 per organization, suggesting that most of the complaints relate to a small number of data users.

Table 9: Number of complaints in the last 12 months	Count	%
0	209	94.6%
1	3	1.4%
2	1	0.5%
3	2	0.9%
5	3	1.4%
10	1	0.5%
1000	1	0.5%
8000	1	0.5%
Total	221	100.0%

The respondents were asked about the primary compliance problem and the most common privacy-related complaint by open-ended questions. In summary, the primary compliance problem most commonly reported was lack of knowledge or education (14 responses), followed by lack of management support (5 responses). As so few organizations reported any privacy-related complaints in the last 12 months, there is no useful summary for the most common complaint.

2.2.6 Knowledge of relevant Mainland China laws and regulations

Table 10 shows the level of knowledge of the Cybersecurity Law (a major law regulating personal information protection, among other things) and the Personal Information Security Specification (PI SS) (a non-binding standard on personal information protection) of Mainland China. More than half of the respondents reported no knowledge (0 on a scale from 0 to 10) of the Cybersecurity law (58.9%) and the PI SS (59.0%).

Table 10: Level of knowledge of relevant Mainland China laws & regulations (0-10)	Cybersecurity Law	%	PI SS	%
0	129	58.9%	128	59.0%
1	5	2.3%	5	2.3%
2	10	4.6%	11	5.1%
3	17	7.8%	13	6.0%
4	15	6.8%	10	4.6%
5	19	8.7%	25	11.5%
6	8	3.7%	6	2.8%
7	7	3.2%	4	1.8%
8	7	3.2%	11	5.1%
9	0	0.0%	1	0.5%
10	2	0.9%	3	1.4%
Total	219	100.0%	217	100.0%

2.2.7 Awareness of the PCPD

Table 11 shows that the level of awareness of the PCPD's publicity materials through different channels. Mass media is the highest (59%), followed by advertisements (other than mass media) (28%), website/social media (25%), publications (24%) and events (12%).

Table 11: PCPD awareness	Mass media	%	Advert	%	Website/ social media	%	Publications	%	Events	%
Yes	135	59%	63	28%	57	25%	54	24%	27	12%
No	90	40%	161	71%	167	74%	169	74%	197	87%
Don't Know / Refuse	2	1%	3	1%	3	1%	4	2%	3	1%
Total	227	100%	227	100%	227	100%	227	100%	227	100%

The respondents were asked about the most helpful form of additional support from the PCPD by an open-ended question. In summary, the most common suggestion was better promotion/publicity, especially online (27 responses), followed by free or online training (13 responses) and better distribution of materials (10 responses).

2.2.8 Support for PDPO Amendments

Tables 12 and 13 show the level of support (on a scale from 0 to 10) for seven possible amendments to the PDPO, namely-

- for significant data breaches, such as the Cathay Pacific case: (1) require organisations to notify the PCPD, (2) give the PCPD the power to require customers to be notified and (3) include financial penalties in the PDPO; and
- for significant misuse of personal data, such as doxxing: (4) require removal of contents from social media platforms and websites that are controlled by entities in Hong Kong, (5) require removal of contents from social media platforms and websites that are controlled by entities overseas, (6) give the PCPD the power of criminal investigation and (7) give the PCPD the power of prosecution for cases like this.

For all the seven possible amendments above, the overall support is quite high, with over 80% supporting at a level of 6 and above for the three data breach related amendments (over 60% giving full support for the notification amendments and over 45% giving full support for the penalties amendment). For the four doxxing related amendments, there is over 60% supporting at a level of 6 and above (around 30% giving full support for all four amendments).

Table 12: Support for data breach amendments	**Notify PCPD**	**%**	**Notify customers**	**%**	**Financial penalties**	**%**
0	2	0.9%	3	1.3%	6	2.7%
1	1	0.4%	0	0.0%	0	0.0%
2	0	0.0%	1	0.4%	1	0.4%
3	1	0.4%	3	1.3%	2	0.9%
4	0	0.0%	0	0.0%	1	0.4%
5	7	3.1%	6	2.7%	26	11.6%
6	9	4.0%	11	4.9%	10	4.5%
7	20	9.0%	20	8.9%	26	11.6%
8	33	14.8%	30	13.3%	34	15.2%
9	13	5.8%	10	4.4%	17	7.6%
10	137	61.4%	141	62.7%	101	45.1%
Total	223	100.0%	225	100.0%	224	100.0%

Table 13: Support for doxxing amendments	Remove HK	%	Remove overseas	%	Criminal investigation	%	Criminal prosecution	%
0	16	7.3%	23	10.7%	23	10.7%	25	11.6%
1	1	0.5%	0	0.0%	1	0.5%	1	0.5%
2	1	0.5%	3	1.4%	4	1.9%	5	2.3%
3	7	3.2%	10	4.7%	12	5.6%	14	6.5%
4	7	3.2%	4	1.9%	4	1.9%	6	2.8%
5	46	21.1%	40	18.6%	35	16.3%	33	15.3%
6	11	5.0%	14	6.5%	15	7.0%	11	5.1%
7	19	8.7%	18	8.4%	25	11.6%	25	11.6%
8	32	14.7%	31	14.4%	22	10.2%	25	11.6%
9	7	3.2%	9	4.2%	10	4.7%	9	4.2%
10	71	32.6%	63	29.3%	64	29.8%	62	28.7%
Total	218	100.0%	215	100.0%	215	100.0%	216	100.0%

The following eleven possible amendments to the PDPO were only included in the online survey, namely, (1) specification of the data retention period, (2) regulation of data processors, (3) clarifying the definition of personal data, (4) adding a legal requirement on privacy accountability, (5) enhancing regulation of sensitive personal data, (6) providing stronger protection for the personal data of children, (7) updating the regulation of cross-boundary/border transfer of personal data, (8) adding the right to be forgotten, (9) adding the right to object to automated decision-making, (10) adding the right to data portability and (11) repealing the data user return scheme. The online survey was completed by 23 members of the Data Protection Officers' Club and 1 respondent from a member of a chamber of commerce. We would expect that these respondents should be relatively well aware of the rationale for the amendments. However, they will not necessarily represent the views of organisations as a whole in Hong Kong.

Tables 14a/b/c show that the level of support (on a scale from 0 to 10) for all the eleven possible amendments to the PDPO was at least 70% (at the level of 6 and above). Clarification of what is personal data, enhanced protections for sensitive personal data and personal data of children had full support from at least 40% of the online survey respondents. Regulation of data processors, privacy accountability, updating the regulations of cross-boundary/border transfer, the right to be forgotten, rights regarding automated decisions and repealing the data user return scheme had full support from at least 30% of the online survey respondents. Retention policy and portability rights had full support from at least 20% of the online survey respondents.

Table 14a: Support other amendments	Retention policy	%	Data processors	%	Personal data definition	%	Accountability	%
0	2	9.1%	1	4.8%	1	4.5%	2	9.5%
1	1	4.5%	0	0.0%	0	0.0%	0	0.0%
2	0	0.0%	0	0.0%	0	0.0%	0	0.0%
3	0	0.0%	0	0.0%	0	0.0%	0	0.0%
4	0	0.0%	0	0.0%	0	0.0%	1	4.8%
5	3	13.6%	2	9.5%	1	4.5%	2	9.5%
6	1	4.5%	0	0.0%	0	0.0%	0	0.0%
7	4	18.2%	3	14.3%	4	18.2%	2	9.5%
8	4	18.2%	6	28.6%	3	13.6%	4	19.0%
9	2	9.1%	1	4.8%	4	18.2%	3	14.3%
10	5	22.7%	8	38.1%	9	40.9%	7	33.3%
Total	22	100.0%	21	100.0%	22	100.0%	21	100.0%

Table 14b: Support other amendments	Sensitive data	%	Enhanced protection for children	%	Cross-boundary/ border transfer	%	Right to be forgotten	%
0	1	4.8%	1	4.8%	3	13.6%	1	4.5%
1	0	0.0%	0	0.0%	0	0.0%	1	4.5%
2	0	0.0%	0	0.0%	0	0.0%	0	0.0%
3	0	0.0%	0	0.0%	0	0.0%	0	0.0%
4	0	0.0%	0	0.0%	0	0.0%	0	0.0%
5	2	9.5%	2	9.5%	2	9.1%	2	9.1%
6	0	0.0%	0	0.0%	1	4.5%	1	4.5%
7	4	19.0%	3	14.3%	2	9.1%	4	18.2%
8	4	19.0%	3	14.3%	3	13.6%	4	18.2%
9	1	4.8%	2	9.5%	3	13.6%	2	9.1%
10	9	42.9%	10	47.6%	8	36.4%	7	31.8%
Total	21	100.0%	21	100.0%	22	100.0%	22	100.0%

Table 14c: Support other amendments	Automated decision right	%	Portability right	%	Repealing data user returns	%
0	1	5.0%	2	10.0%	1	5.3%
1	0	0.0%	0	0.0%	0	0.0%
2	0	0.0%	0	0.0%	0	0.0%
3	0	0.0%	1	5.0%	1	5.3%
4	0	0.0%	0	0.0%	0	0.0%
5	2	10.0%	2	10.0%	2	10.5%
6	3	15.0%	0	0.0%	0	0.0%
7	3	15.0%	4	20.0%	5	26.3%
8	2	10.0%	5	25.0%	1	5.3%
9	2	10.0%	2	10.0%	3	15.8%
10	7	35.0%	4	20.0%	6	31.6%
Total	20	100.0%	20	100.0%	19	100.0%

2.2.9 Implementation stage and privacy risks of new technologies

From the online survey, we have information about the stage of implementation of Artificial Intelligence ("AI"), Big Data, Blockchain, Cloud Computing and Internet of Things (IoT) and about their perceived privacy risk as regards excessive collection of personal data, transparency, change of use, security and unnecessary retention of personal data. Table 15 summarizes the stage of implementation, which shows Cloud Computing (50% implemented) and IoT (41.7% implemented) are furthest ahead. Again, as the online survey was mainly completed by members of the Data Protection Officers' Club of the PCPD, we would expect that these respondents should be relatively well aware of the privacy risks of these new technologies.

Table 15 Tech implementation	AI	%	Big Data	%	Blockchain	%	Cloud Computing	%	IoT	%
Not considered	10	41.7%	8	33.3%	13	54.2%	3	12.5%	8	33.3%
Not implemented yet	7	29.2%	9	37.5%	8	33.3%	9	37.5%	6	25.0%
Implemented	7	29.2%	7	29.2%	3	12.5%	12	50.0%	10	41.7%
Total	24	100.0%	24	100.0%	24	100.0%	24	100.0%	24	100.0%

Tables 16-20 summarize the perceived privacy risks, so we can see that AI and Big Data are generally seen to involve high privacy risk, specifically as regards excessive collection of personal data (64.3% for AI, 62.5% for Big Data), transparency on personal data processing (57.1% for AI, 50.0% for Big Data), change of use of personal data (57.1% for AI, 50.0% for Big Data), unnecessary retention of personal data (47.1% for AI, 43.8% for Big Data) and data security (50.0% for AI, 43.8% for Big Data).

Table 16 Excessive collection	AI	%	Big Data	%	Blockchain	%	Cloud Computing	%	IoT	%
High risk	9	64.3%	10	62.5%	4	36.4%	5	23.8%	3	18.8%
Low risk	2	14.3%	2	12.5%	4	36.4%	10	47.6%	4	25.0%
No	2	14.3%	4	25.0%	2	18.2%	6	28.6%	8	50.0%
Don't Know	1	7.1%	0	0.0%	1	9.1%	0	0.0%	1	6.3%
Total	14	100.0%	16	100.0%	11	100.0%	21	100.0%	16	100.0%

Table 17 Transparency	AI	%	Big Data	%	Blockchain	%	Cloud Computing	%	IoT	%
High risk	8	57.1%	8	50.0%	4	36.4%	7	33.3%	2	12.5%
Low risk	5	35.7%	4	25.0%	5	45.5%	10	47.6%	7	43.8%
No	1	7.1%	3	18.8%	2	18.2%	4	19.0%	6	37.5%
Don't Know	0	0.0%	1	6.3%	0	0.0%	0	0.0%	1	6.3%
Total	14	100.0%	16	100.0%	11	100.0%	21	100.0%	16	100.0%

Table 18 Change of use	AI	%	Big Data	%	Blockchain	%	Cloud Computing	%	IoT	%
High risk	8	57.1%	8	50.0%	3	27.3%	5	23.8%	2	12.5%
Low risk	3	21.4%	2	12.5%	5	45.5%	8	38.1%	4	25.0%
No	2	14.3%	5	31.3%	3	27.3%	8	38.1%	9	56.3%
Don't Know	1	7.1%	1	6.3%	0	0.0%	0	0.0%	1	6.3%
Total	14	100.0%	16	100.0%	11	100.0%	21	100.0%	16	100.0%

Table 19 Unnecessary retention	AI	%	Big Data	%	Blockchain	%	Cloud Computing	%	IoT	%
High risk	8	47.1%	7	43.8%	4	36.4%	7	33.3%	2	12.5%
Low risk	3	17.6%	4	25.0%	4	36.4%	7	33.3%	8	50.0%
No	3	17.6%	3	18.8%	2	18.2%	6	28.6%	5	31.3%
Don't Know	3	17.6%	2	12.5%	1	9.1%	1	4.8%	1	6.3%
Total	17	100.0%	16	100.0%	11	100.0%	21	100.0%	16	100.0%

Table 20 Security	AI	%	Big Data	%	Blockchain	%	Cloud Computing	%	IoT	%
High risk	7	50.0%	7	43.8%	4	36.4%	9	42.9%	4	25.0%
Low risk	6	42.9%	6	37.5%	5	45.5%	9	42.9%	8	50.0%
No	1	7.1%	2	12.5%	2	18.2%	2	9.5%	3	18.8%
Don't Know	0	0.0%	1	6.3%	0	0.0%	1	4.8%	1	6.3%
Total	14	100.0%	16	100.0%	11	100.0%	21	100.0%	16	100.0%

Chapter 3 Summary and Recommendations

3.1 Methodology

A total of 227 responses were obtained, 203 via a telephone survey and 24 via an online survey. While the survey can probably not be projected to the entire population of data users in Hong Kong, given the low response rate, it represents the views of a wide-ranging set of data users, in terms of both industry sector and number of Hong Kong employees and should have considerable value in elaborating the views of data users on data protection and privacy.

3.2 Summary of the Data User Survey

Demographic profile of respondents

The combined sample is broadly representative, as it consists of responses from 13 different sectors. The sample has not been weighted to match the data of the Census and Statistics Department, as the low response rate makes it questionable whether we have a statistically representative result. However, the wide range of sectors included allow us to see the range of views across different sectors. Although small establishments (1-9 employees in Hong Kong) are the most common in our sample, we have representation across all sizes of establishments.

Privacy Management Programme

For the level of understanding of PMP, the most common answer was no understanding at all (a rating of 0 on a scale from 0 to 10), by 25% of respondents, however 37.9% rated their level as 6 or above. For the stage of implementation of PMP, the most common stage is no implementation at all (a rating of 0), by 27.3%, however 49.7% reported the stage as 6 or above. The primary benefit of PMP most commonly reported (70 responses) was better data protection, followed by better compliance (5 responses), with all other responses only occurring once or twice. The primary difficulty in implementation of PMP most commonly reported was difficulty in educating employees (7 responses), followed by lack of management support (4 responses) and lack of clarity in PMP (3 responses).

Data Protection Officer

Only 17.6% of respondents have a DPO.

Privacy Impact Assessment

Only 14.1% of respondents have undertaken a PIA.

Compliance and complaints

For the difficulty that respondents have with compliance with the PDPO, the most common answer is 5 on a scale from 0 to 10, by 21.4% of respondents, with 21.4% reporting the difficulty as 6 to 10. For the number of privacy-related complaints that respondents have had received in the last 12 months, the overwhelming majority (94.6%) reporting no complaints, with a mean number of complaints of about 40 per organization, suggesting that most of the complaints relate to a small number of data users.

Knowledge of relevant Mainland China laws and regulations

Most respondents do not have good knowledge of the two major Mainland China laws and regulations on personal data protection, with more than half reporting no knowledge (0 on a scale from 0 to 10) of the Cybersecurity Law (58.9%) and the Personal Information Security Specification (59.0%).

Awareness of the PCPD

Among the different publicity channels used by the PCPD, awareness of the PCPD publicity materials through mass media, advertisements (other than mass media), publications, website/social media and events is highest for mass media (59%), followed by advertisements (other than mass media) (28%), website/social media (25%), publications (24%) and events (12%). For the most helpful form of additional support from the PCPD, the most common suggestion was better promotion/publicity, especially online (27 responses); followed by free or online training (13 responses) and better distribution of materials (10 responses).

Support for possible amendments to the PDPO

The data user survey covered seven major possible amendments to the PDPO. For significant data breaches (such as the Cathay Pacific case), the amendments considered were: (1) requiring organisations to notify the PCPD, (2) giving the PCPD the power to require customers to be notified and (3) including financial penalties in the PDPO. For significant misuse of personal data (such as doxxing), the amendments considered were: (4) requiring removal of contents from social media platforms and websites that are controlled by entities in Hong Kong, (5) require removal of contents from social media platforms and websites that are controlled by entities overseas, (6) giving the PCPD the power of criminal investigation and (7) giving the PCPD the power of prosecution for cases like this. The support for these seven amendments is quite high, with over 80% supporting at a rating of 6 and above (on a scale from 0 to 10) for the three data breach related amendments (over 60% giving full support for the notification

amendments and over 45% giving full support for the penalties amendment) and over 60% supporting at a rating of 6 and above for the four doxxing related amendments (around 30% giving full support for all four amendments).

The online survey covered another eleven possible amendments to the PDPO, covering (1) specification of the data retention period, (2) regulation of data processors, (3) clarifying the definition of personal data, (4) adding a legal requirement on privacy accountability, (5) enhancing regulation of sensitive personal data, (6) providing stronger protection for the personal data of children, (7) updating the regulation of cross-boundary/border transfer of personal data, (8) adding the right to be forgotten, (9) adding the right to object to automated decision-making, (10) adding the right to data portability and (11) repealing the data user return scheme. As the online survey was mainly completed by members of the Data Protection Officers' Club of the PCPD, we would expect that these respondents should be relatively well aware of the rationale for these amendments. From the online survey, the level of support for all eleven possible amendments to the PDPO was at least 70% supported at a rating of 6 and above (on a scale from 0 to 10). Clarification of what is personal data, enhanced protections for sensitive personal data and children's personal data had full support from at least 40%. Regulation of data processors, privacy accountability, updating the cross-boundary/border protections, the right to be forgotten, rights regarding automated decisions and repealing the data user return scheme had full support from at least 30%. Retention policy and portability rights had full support from at least 20% of online survey respondents.

Implementation stage and privacy risks of new technologies

From the online survey, we have information about the stage of implementation of Artificial Intelligence (AI), Big Data, Blockchain, Cloud Computing and Internet of Things (IoT) and about their perceived privacy risk as regards excessive collection of personal data, transparency, change of use, security and unnecessary retention of personal data. For the stage of implementation, Cloud Computing (50% implemented) and IoT (41.7% implemented) are furthest ahead. Again, as the online survey was mainly completed by members of the Data Protection Officers' Club, we would expect that these respondents should be relatively well aware of the privacy risks of these new technologies. The respondents reported that AI and Big Data are generally seen to involve high privacy risk, specifically as regards excessive collection of personal data (64.3% for AI, 62.5% for Big Data), transparency in personal data processing (57.1% for AI, 50.0% for Big Data), change of use of personal data (57.1% for AI, 50.0% for Big Data), unnecessary retention of personal data (47.1% for AI, 43.8% for Big Data) and data security (50.0% for AI, 43.8% for Big Data).

3.3 Recommendations

Privacy Management Programme

While more than a third of the respondents reported their level of understanding of PMP as 6 or above, around a quarter had no knowledge at all, suggesting a broader need for educating organizations about the concepts of PMP, so that they at least understand its relevance. The stage of implementation matches up, with about a quarter having no implementation at all. However, it is clear that most respondents clearly understood that the primary benefit of PMP is better data protection. The primary difficulty in implementing PMP most commonly reported was difficulty in educating employees, again highlighting the need for additional training.

Data Protection Officer and Privacy Impact Assessment

Less than 20% of respondents have a DPO or undertaken a PIA, suggesting a need to persuade organizations of the value of a DPO and the PIA process.

Compliance and complaints

The level of difficulty in compliance with the PDPO reported is very variable, indicating the need for identifying the sectors with greater difficulty in compliance (the PCPD data on complaints is probably a sound basis for this). As the overwhelming majority reported no privacy-related complaints, this suggests that most of the complaints relate to a small number of data users and hence the continuing need for a targeted approach.

Knowledge of Mainland China laws and regulations on data protection

The majority of respondents reported no knowledge of the two major Mainland China laws and regulations on data protection, though the survey does not allow us to check whether that knowledge is relevant, so targeted training may arguably be required.

Awareness of the PCPD

Awareness of the PCPD publicity materials through mass media, advertisements (other than mass media), publications, website/social media and events is highest for mass media, followed by advertisements (other than mass media), website/social media, publications and events, suggesting the need for some consideration of updating the publicity strategy, especially given that the most common request for additional support from the PCPD was better promotion/publicity, especially online; followed by free or online training and better distribution of materials.

Support for possible amendments to the PDPO

The level of support for the seven possible amendments to the PDPO relating to significant data breaches and significant misuse of personal data (such as doxxing) was high, especially for notification of the PCPD and customers and financial penalties for significant data breaches, such as the Cathay Pacific case, although the level of support is less for the four doxxing related amendments.

The online survey covered another eleven possible amendments to the PDPO. As the online survey was mainly completed by members of the Data Protection Officers' Club, it is important to be cautious in interpreting the high level of support for these eleven possible amendments. However, clarification of what is personal data, enhanced protections for sensitive personal data and personal data of children had the highest level of full support, suggesting that they could be prioritized in that informed data users are more likely to support these amendments. Regulation of data processors, privacy accountability, updating the cross-boundary/border protections, the right to be forgotten, rights regarding automated decisions and repealing data user returns has a lower level of support. Retention policy and portability right had the weakest level of full support.

Implementation stage and privacy risks of new technologies

From the online survey, we see that Cloud Computing and IoT are furthest ahead in implementation. However, AI and Big Data are generally seen to involve high privacy risk by about half of respondents, as regards excessive collection of personal data, transparency in personal data processing, change of use of personal data, unnecessary retention of personal data and data security, suggesting that the high privacy risks might be one reason why these technologies are behind in implementation and hence suggesting that the PCPD guidance is most important in these domains.

3.4 Limitations of the data user survey

The response rate for the online survey was low, so it is unclear to what extent the responses to the questions only included in the online survey are representative of data users.

The telephone survey sample frame used the Central Register of Establishments, which includes commercial undertakings, semi-government organisations and non-profit making bodies, but not the Government of the HKSAR.

The online survey sample frame relied mainly on membership of the PCPD’s Data Protection Officers' Club, which in principle covers all establishments, including the Government of the HKSAR, but is likely to over represent larger and more sophisticated establishments, who have the resources to hire a data protection officer.

Appendix A: Questionnaire for Data User Survey

Survey of Data User Attitudes on Personal Data Privacy Protection 2020
資料使用者對保障個人資料私隱的態度調查 2020

Bilingual Questionnaire

Part I: Introduction (Online version)

第一部份: 介紹

Social Sciences Research Centre of the University of Hong Kong is commissioned by the Office of the Privacy Commissioner for Personal Data to conduct a survey on personal data protection in HK. We would like to invite someone responsible for personal data protection or human resources in your company to take part in this survey, which would take you about 30 minutes. The findings will be used by the office of the Privacy Commissioner for Personal Data for gauging the views of personal data users on matters related to personal data privacy. I would like to stress that all information collected will remain strictly confidential. Individual details will not be disclosed or identifiable from this survey. If you have any questions or concerns about the research, please contact HKUSSRC at 3917-1600. If you have questions about your rights as a research participant, please contact the Human Research Ethics Committee for Non-Clinical Faculties, HKU (2241-5267).

香港大學社會科學研究中心受個人資料私隱專員公署委託進行一項有關在香港保護個人資料的意見調查。我們想邀請 貴公司負責保護個人資料或人力資源的人員參加此調查，這大約需時 30 分鐘。調查結果將被個人資料私隱專員公署用作評估公眾對保護個人資料相關問題的看法。所有收集到的資料會絕對保密，任何在這次調查收集到的個人資料都不會被公開或被識辨得到。如果你對這次調查有任何查詢或意見，請致電 3917-1600 向香港大學社會科學研究中心查詢。如果你想知道更多有關研究參與者的權益，請致電 2241-5267 向香港大學非臨床研究操守委員會查詢。

Part I: Introduction (telephone survey version)

第一部份: 介紹

Good afternoon/evening! My name is (surname). I am an interviewer at the Social Sciences Research Centre, University of Hong Kong, conducting a survey for the office of the Privacy Commissioner for Personal Data. I would like to contact someone responsible for personal data protection or human resources in your company.

午安/晚安。我姓x，我係香港大學社會科學研究中心嘅訪問員。我哋現正為個人資料私隱專員公署進行一項電話調查，我哋希望聯絡 貴公司負責保護個人資料或人力資源嘅人員。

[v1 Telephone #]
[v1 電話號碼 #]
[v2 Interviewer #]
[v2 訪問員 #]

<respondent selection for data users to ensure they are suitable to answer the questions>

<訪問員:請確保選出的受訪者是資料使用者，並適合回答問題。>

Good morning/afternoon/evening! My name is (surname). I am an interviewer at the Social Sciences Research Centre, University of Hong Kong, conducting a survey for the office of the Privacy Commissioner for Personal Data. I would like to ask for your opinion on personal data protection in HK, which would only take about 15 minutes. The findings will be used by the office of the Privacy Commissioner for Personal Data for gauging the views of personal data users on matters related to personal data privacy. Our conversation may be audio-recorded for further data checking. I would like to stress that all information collected will remain strictly confidential. Individual details will not be disclosed or identifiable from this survey. If you have any questions or concerns about the research, please contact HKUSSRC at 3917-1600. If you have questions about your rights as a research participant, please contact the Human Research Ethics Committee for Non-Clinical Faculties, HKU (2241-5267).

早晨/午安/晚安。我姓 x，我係香港大學社會科學研究中心嘅訪問員。我哋現正為個人資料私隱專員公署進行一項電話調查，希望收集有關你對香港保護個人資料嘅意見。整個

訪問需時大約 15 分鐘。調查結果將被個人資料私隱專員公署用作評估公眾對保護個人資料相關問題嘅睇法。為方便日後核對資料，訪問會被錄音。 所有收集到嘅資料會絕對保密，任何喺呢次調查所收集到嘅個人資料都唔會被公開或被識辨得到。如果你對呢項調查有任何查詢或意見，請致電 3917-1600 向香港大學社會科學研究中心查詢。 如果你想知道更多有關研究參與者嘅權益，請致電 2241-5267 向香港大學非臨床研究操守委員會查詢。

We would like to invite you to take part in the survey. Do you agree to the audio recording? Do you agree to participate in this survey?

我地想邀請你參與呢項調查。請問你同意被錄音嘛，你同唔同意參與呢項調查?

If agree, interview starts, else interview ends, thank respondent.

如同意，訪問員開始，否則訪問結束，多謝被訪者

Demographics: 背景

The following questions are about your company for analysis purposes only.

以下問題是關於你的公司資料並只會用作分析用途

Q1. Which industry sector does your company belong to?

貴公司屬於哪個行業?

1. Manufacturing 製造業
2. Electricity and gas supply, and waste management 電力和氣體供應，及廢物管理
3. Construction 建造業

4. Import/export trade and wholesale 進出口貿易及批發
5. Retail 零售業
6. Transportation, storage, postal and courier services 運輸、倉存、郵政及快遞服務
7. Accommodation and food services 住宿及餐飲服務
8. Information and communications 資訊及通訊
9. Financing and insurance 金融及保險
10. Real estate 房地產
11. Professional and business services 專業及商務服務
12. Social and personal services 社會及個人服務
13. Travel 旅遊業
14. Other:_____ 其他；_____

Q2. Approximately how many employees does your company have in HK?

貴公司在香港擁有大約幾多名員工?

1. 1-9
2. 10-19
3. 20-49
4. 50-100
5. Over 100 100 以上

(Online survey only for Q3)

Q3a. I would like to ask about the adoption by your company of and concern about privacy risks of some new information and communications technology (ICT) for processing personal data:

我想了解 貴公司有沒有採用一些新的資訊及通訊科技來處理個人資料，以及對當中的私隱風險之關注:

Has your company considered adopting:

貴公司有沒有考慮採用:

(a) Artificial Intelligence (Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions.)

人工智能 (人工智能 (AI) 是指在機器中模擬人類智慧，這些機器被程式設計為像人類一樣思考並模仿他們的動作。)

1. Not considered 沒有考慮
2. Considered but not yet implemented 有考慮但未實施
3. Implemented 已經實施

(b) Big Data (Big data is a combination of structured, semi-structured and unstructured data collected by organizations that can be mined for information and used in machine learning projects, predictive modeling and other advanced analytics applications.)

大數據 (大數據是組織收集結構化、半結構化和非結構化數據的組合，這些數據可用於機器學習項目、預測模型和其他高級分析應用程式。)

1. Not considered 沒有考慮
2. Considered but not yet implemented 有考慮但未實施

3. Implemented 已經實施

(c) Blockchains (Blockchain is a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network.)

區塊鏈 (區塊鏈是一個數位資料庫，包含資訊(如金融交易記錄)，可在大型分散、可公開的網路中同時使用和共用。)

1. Not considered 冇考慮
2. Considered but not yet implemented 有考慮但未實施
3. Implemented 已經實施

(d) Cloud computing (Cloud Computing is an Internet-based computing method, in which shared hardware and software resources and information can be provided to various terminals and other devices of computers on demand. Also, using computer infrastructure provided by service providers for operation and resources.)

雲端運算 (雲端運算是一種基於網際網路的運算方式，通過這種方式，共享的軟硬體資源和資訊可以按需求提供給電腦各種終端和其他裝置，使用服務商提供的電腦基建作運算和資源。)

1. Not considered 沒有考慮
2. Considered but not yet implemented 有考慮但未實施
3. Implemented 已經實施

(e) Internet of Things (IoT) (i.e., connecting devices and equipment over the Internet. IoT is not just to connect things together, it is more important to allow devices and equipment to interconnect and exchange data and make required commands.)

物聯網 (即通過互聯網把裝置和設備連在一起，物聯網不只是把東西串起來，更重要的是讓裝置和設備之間可以互聯互通與互相交換資料並作出所需的指令。)

1. Not considered 沒有考慮
2. Considered but not yet implemented 有考慮但未實施
3. Implemented 已經實施

Q3b. For each area, if considered or implemented, then do you believe there is any privacy risk as regards the following issues:

對於每一個新的資訊及通訊科技，如果有考慮或已經實施,請問你認為會不會存在以下的私隱風險呢?

i) Excessive collection of personal data 過度收集個人資料

1. Yes, and high risk 會，且風險高
2. Yes, but low risk 會，但風險低
3. No 不會
4. Don't Know 不知道

ii) Lack of transparency and explain ability on personal data processing

就如何處理個人資料缺乏透明度和詳細解釋

1. Yes, and high risk 會，且風險高
2. Yes, but low risk 會，但風險低
3. No 不會
4. Don’t Know 不知道

iii) Change of use of personal data without consent of the individuals concerned
未經有關個人同意下更改個人資料的用途

1. Yes, and high risk 會，且風險高
2. Yes, but low risk 會，但風險低
3. No 不會
4. Don’t Know 不知道

iv) Unnecessary retention of personal data 不必要地保留個人資料

1. Yes, and high risk 會，且風險高
2. Yes, but low risk 會，但風險低
3. No 不會
4. Don’t Know 不知道

v) Data security risk 資料保安風險

1. Yes, and high risk 會，且風險高
2. Yes, but low risk 會，但風險低
3. No 不會
4. Don't Know 不知道

Q4. How well do you understand the concept of Privacy Management Programme (PMP) on a scale from 0 to 10? (0 - totally do not understand and 10 - totally understand)

請問你對私隱管理計劃的概念有幾了解?

(請用 0 至 10 分表示。0 分代表完全不了解，10 分代表完全了解。)

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

If rate higher than 0, then ask Q5-Q7

如果高過 0 分，請問 Q5-Q7

Q5. What do you see as the primary benefit of PMP?

你認為私隱管理計劃(PMP) 的主要優勢是甚麼?

_____

Q6. What do you see as the primary difficulty of implementing PMP?

你認為實施私隱管理計劃(PMP) 的主要困難是甚麼?

_____

Q7. What is the stage of implementation of PMP in your company from 0-10? (0 - not yet implemented and 10 - fully implemented)

請問 貴公司實施私隱管理計劃(PMP)到哪個階段? 請用 0 至 10 分表示。0 分代表完全未實施，10 分代表已完善地實施。

1. 0－10 0-10
2. No idea / don’t know 不知道
3. Refuse to answer 拒絕回答

Q8. Does your company have any data protection officer(s)?

請問 貴公司有沒有個人資料保障主任?

1. Yes 有
2. No 沒有
3. Don’t Know 不知道

Q9. Has your company undertaken any Privacy Impact Assessments (PIA) for its operational activities?

請問 貴公司有沒有就你們的營運活動進行過任何有關私隱影響的評估 (PIA)？

1. Yes 有
2. No 沒有
3. Don’t Know 不知道

Q10. How difficult is it for your company to comply with the Personal Data (Privacy) Ordinance on a scale from 0-10? (0 - no difficulty at all and 10 - very difficult)

對於 貴公司要遵守《個人資料(私隱)條例》會有幾困難? 請用 0 至 10 分表示。

(0 分代表完全沒有困難，10 分代表非常困難。)

1. 0－10 0-10
2. No idea / don’t know 不知道

3. Refuse to answer 拒絕回答

Q11. What is the biggest problem in compliance?

請問要遵守的最大困難是甚麼?

_____

Q12. Approximately how many privacy-related complaints has your company received in the last 12 months?

在過去 12 個月中， 貴公司收到幾多個與私隱相關的投訴?

_____個

Q13. What was the most common grievance of privacy-related complaint?

私隱投訴中最常見的不滿是甚麼?

_____

Q14. What is your level of familiarity on a scale from 0 to 10 with the personal data protection-related laws and regulations in mainland China, specifically:
(0 - totally unfamiliar and 10 - complete familiarity)

請用 0 至 10 分表示，你對於中國有關保障個人資料的相關法律及規例的熟悉程度，

特別是:

(0 分代表完全唔熟悉，10 分代表完全熟悉。)

a) the Cybersecurity Law and;

網絡安全法及;

1. 0－10 0-10
2. No idea / don't know 不知道

3. Refuse to answer 拒絕回答

b) the Personal Information Security Specification

個人信息安全規範

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

Channels for learning about the office of the Privacy Commissioner for Personal Data (PCPD) and the effectiveness and trustworthiness of the PCPD

了解個人資料私隱專員公署的途徑、其工作效率及**可靠程度**

Have you been made aware of the work of the Office of the Privacy Commissioner for Personal Data (PCPD) through the following channels?

你有沒有曾經透過以下的途徑留意到個人資料私隱專員公署的工作?

Q15. Mass media (e.g. news on TV, newspaper and radio or advertisements)

大眾媒體（如電視、報紙及電台的新聞或廣告）

1. Yes 有
2. No 沒有
3. No idea 不知道
4. Refuse to answer 拒絕回答

Q16. Advertisements other than mass media (e.g. buses, trains/trams, other advertising panels)

大眾媒體以外的廣告（如巴士、港鐵/電車及其他廣告板）

1. Yes 有

2. No 沒有

3. No idea 不知道

4. Refuse to answer 拒絕回答

Q17. PCPD's publications (e.g. guidance notes, pamphlets, fact sheets and codes of practice)

個人資料私隱專員公署的刊物（如指引、小冊子，資訊單張和實務守則）

1. Yes 有

2. No 沒有

3. No idea 不知道

4. Refuse to answer 拒絕回答

Q18. PCPD website and social media

個人資料私隱專員公署的網站及社交媒體

1. Yes 有

2. No 沒有

3. No idea 不知道

4. Refuse to answer 拒絕回答

Q19. PCPD publicity programmes (e.g. seminars, workshops and exhibitions)

個人資料私隱專員公署的推廣活動（例如講座、工作坊及展覽）

1. Yes 有

2. No 沒有

3. No idea 不知道

4. Refuse to answer 拒絕回答

Q20. What additional form of support from the PCPD would be most helpful?

對你來說，個人資料私隱專員公署提供哪些額外的支援是最有幫助呢?

Amendments to PDPO

修改《個人資料（隱私）條例》

The Government is currently considering making changes to the Personal Data (Privacy) Ordinance (PDPO). I would like to ask you about some possible changes to the law and the extent to which you support those changes on a scale from [0-10], where 0 means no support at all to 10 means fully support these changes.

政府目前正在考慮對《個人資料（隱私）條例》進行修改。請問你對一些修改法例的可能之看法，以及你有幾大程度上支持這些修改? 以[0-10]表示，其中 0 表示完全不支持，10 表示完全支持這些修改。

You may be aware that Cathay Pacific was hit by a data leak in 2018, affecting about 9.4 million passengers, including passport numbers, email address and credit card data. Cathay did not disclose the breach to the PCPD for more than 6 months after it first identified intrusion to its systems and the PDPO does not currently require notification of data breaches and does not currently have financial penalties for such a breach.

你可能有留意到，國泰航空曾於 2018 年發生資料外洩，有多達 940 萬乘客受影響，涉及的個人資料包括護照號碼，電郵地址和信用卡資料。國泰在首次發現系統被入侵後，有長達六個月沒有向個人資料私隱專員公署通報有關事故；並且目前《個人資料(私隱)條例》沒有規定就資料外洩作出通報，及沒有對資料外洩處以罰款。

How much would you support a change in the law to:

你有幾大程度會支持修改法律以:

Q21.Require organisations to notify the PCPD of significant data breaches like this?

要求機構將此類重大資料外洩事故通知個人資料私隱專員公署?

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

Q22. Give the PCPD the power to require customers to be notified of significant data breaches like
this?

給予個人資料私隱專員公署有權要求將此類重大資料外洩事故通知客戶?

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

Q23. Include financial penalties in the law for significant data breaches like this?

在法例中規定可對此類重大資料外洩事故處以罰款?

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

You may be aware of numerous cases of doxxing in the last year. Currently the PCPD does not have power to carry out criminal investigation or initiate prosecution themselves. At present,

criminal investigations are conducted by the Police, and prosecutions, if so required, are initiated by the Department of Justice. (Doxxing means where the personal data of individuals was disclosed publicly in order to encourage taking action against those individuals and their families)

你可能有留意到，上年發生了大量「起底」的個案。目前，個人資料私隱專員公署是沒有權力自行進行刑事調查或提起訴訟。現時，刑事調查是由警方進行，如果有必要，則由律政司提出訴訟。 (「起底」的意思是公開個別人士的個人資料以鼓吹採取針對這個人及他的家人之行動。)

How much would you support a change in the law to give the PCPD the power to:

你有幾大程度上支持修改法例以給予個人資料私隱專員公署有權:

Q24. Require the removal of doxxing contents from social media platforms and websites that are under Hong Kong control

要求從受香港控制的社交媒體平台和網站刪除有關「起底」的內容

1. 0－10 0-10
2. No idea / don’t know 不知道
3. Refuse to answer 拒絕回答

Q25. Require the removal of doxxing contents from social media platforms and websites that are under overseas control (e.g. Facebook and Google)

要求從受海外控制的社交媒體平台和網站刪除有關「起底」的內容（例如 Facebook 和 Google）

1. 0－10 0-10
2. No idea / don’t know 不知道

3. Refuse to answer 拒絕回答

Q26. Carry out criminal investigation of significant misuse of personal data like this?

對這類重大濫用個人資料的行為進行刑事調查

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

Q27. Initiate prosecution of significant misuse of personal data like this?

對這類重大濫用個人資料的行為提起訴訟

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

There are some other possible amendments to PDPO, which I would also like to ask you about your level of support on a scale from 0-10 (0 - no support at all and 10 - fully support):

另外，還有一些其他修改《個人資料（私隱）條例》的可能性，請問你對這些修改的支持程度，請用 0 至 10 分表示。 (0 表示完全不支持， 10 表示完全支持這些修改)

(Remaining questions are online survey only)

Q28. Data retention period – Currently the PDPO only requires retaining personal data for not longer than is necessary, without specifying the retention period. The possible amendment is to require a data user to formulate and disclose a clear retention policy which specifies a retention period for the personal data collected. The rationale is that the longer personal data is retained, the higher the privacy risk.

保留個人資料的期限 - 目前，《個人資料（私隱）條例》只要求保留個人資料的時間不超過實際所需，並沒有指明保留的期限。有關修改可能是，要求資料使用者去訂立及披露一個清晰的保留政策，指明所收集的個人資料的保留期限。而理由是個人資料的保留期越長，私隱風險就越高。

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

Q29. Regulation of data processors – Currently the PDPO does not regulate data processors. The possible amendment is to impose legal obligations on data processors on data retention, data security and data breach notification while the rationale is that outsourcing of data processing work to other service providers has become more common. Regulating data processors will strengthen personal data protection and pose a fairer sharing of responsibilities between data users and data processors.

規管資料處理者 - 目前《個人資料（私隱）條例》並未對資料處理者進行規管。有關修改可能是，對資料處理者施加有關資料保留、資料安全和就資料外洩作出通知的法律責任，而理由是將資料處理工作外判給其他服務供應商已變得更普遍。對資料處理者進行規管，將會加強個人資料保障及能夠讓資料使用者和資料處理者更公平地分擔責任。

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

Q30. Definition of personal data – the possible amendment is to clarify the definition of "personal data" under the PDPO to cover information relating to an "identifiable" natural person (currently it only includes the data that can be practicably used to ascertain the identity of an individual), the rationale is that a clearer definition will provide stronger protection to personal data privacy in this digital age and minimise the dispute on whether a piece of data is personal data.

個人資料的定義- 有關修改可能是，將《個人資料（私隱）條例》下有關「個人資料」 的定義釐清，以涵蓋與「可被識別」的人有關的資料 (目前只是包括可用於確定某人身份的資料)，理由是在這個數碼時代，更清晰的定義將會為個人資料私隱提供更強的保障，並減少對於某些資料是否屬於個人資料的爭議。

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

Q31. Legal requirement on privacy accountability – the possible amendment is to require data users to implement policy and measures to facilitate compliance with the PDPO, including appointing data protection officers, the rationale is that data users are in the best position to develop appropriate measures to address privacy risks, without significantly compromising their business objectives and legitimate interests; prevention is better than cure.

對私隱責任的法例要求 – 有關修改可能是，要求資料使用者實施政策和措施，以助遵守 《個人資料（私隱）條例》，包括委任資料保障主任，理由是資料使用者是最適當人選制定合適的措施以解決各種私隱風險，而不會嚴重損害公司業務和合法利益，是預防勝於治療。

1. 0－10 0-10
2. No idea / don't know 不知道

3. Refuse to answer 拒絕回答

Q32. Enhanced regulation on sensitive personal data – the possible amendment is to define "sensitive personal data" and introduce stronger regulation on the collection and use of sensitive personal data, such as requiring explicit consent by the data subjects. The rationale is that collection and use of sensitive personal data may inflict greater harm on the data subjects, such as stigmatisation and discrimination.

加強監管敏感個人資料 – 有關修改可能是，首先界定「敏感個人資料」定義，及對敏感個人資料的收集和使用實施更嚴格的監管，例如要求向資料當事人徵取明確同意，理由是收集和使用敏感個人資料是可能對資料當事人造成較重大的傷害，例如被負面標籤和歧視。

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

Q33. Stronger protection on children's personal data – the possible amendment is to introduce stronger regulation on the collection and use of children's personal data during online activities, such as requiring parental consent. The rationale is that children are considered more susceptible to advertising techniques and crooked materials online.

加強保障兒童個人資料 – 有關修改可能是，加強監管於網上活動時所收集及使用的兒童個人資料，如要求家長同意，理由是兒童會更容易受到網上廣告技巧和歪曲材料的影響。

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

Q34. Cross-border / cross-boundary transfer of personal data – the possible amendments are to repeal the "white list" for transfer under s.33(2)(a) of the PDPO; recognising privacy certification as a basis for transfer; and requiring data users to notify data subjects about the place to where the personal data will be transferred; implementing s.33 of the PDPO after the amendments. The rationale is that to maintain and update the "white list" will create a lot of challenges due to rapid change in overseas data protection laws; privacy certification is increasingly popular internationally as one of the legal bases for cross-border / boundary data transfer.

跨境/邊界個人資料轉移 – 有關修改可能是，首先廢除《個人資料（私隱）條例》第 33(2)(a) 條下的「白名單」資料轉移機制，及認可私隱認證作為資料轉移的依據，並要求資料使用者通知當事人有關其個人資料將會被轉移到的地點，並在修改條例後，實施《個人資料（私隱）條例》第 33 條。理由是要維持及更新「白名單」將會面對很多挑戰，因為海外保護資料的法律迅速改變，在國際上，私隱認證越來越受歡迎，也被認可為跨境/邊界個人資料轉移的法律依據之一。

1. 0－10 0-10
2. No idea / don't know 不知道
3. Refuse to answer 拒絕回答

Q35. Right to be forgotten - the possible amendment is to give data subjects the right to demand data users to erase their personal data where the personal data is no longer necessary and the rationale is that retention of unnecessary personal data by data users may create higher privacy risk to individuals.

被遺忘權 - 有關修改可能是，在個人資料不再有需要的情況下，讓資料當事人有權要求資料使用者刪除其個人資料，理由是資料使用者保留不必要的個人資料，可能會令當事人帶來更高的私隱風險。

1. 0－10 0-10
2. No idea / don’t know 不知道
3. Refuse to answer 拒絕回答

Q36. Right to object to automated decision-making – the possible amendment is to require data users to notify data subjects the existence of automated decision-making; giving data subjects the right to object to automated decisions which produce legal effects concerning them or significantly affect them, and the right to obtain human intervention on the part of the data user. The rationale is that automated decisions are inherently risky because the information used in deriving the decisions may be inaccurate or incomplete and the algorithms may be defective or biased.

有權反對自動決策 – 有關修改可能是，當存在(人工智能及機器)自動決策時，要求資料使用者通知資料當事人；當自動決策可對當事人產生具法律效力的或嚴重的影響時，賦予當事人有權反對自動決策，及有權要求資料使用者以人為干預有關決策，理由是自動決策具有固有的風險，因為衍生決策所使用的資訊可能不準確或不完整，演算方法可能有缺陷或有偏見。

1. 0－10 0-10
2. No idea / don’t know 不知道
3. Refuse to answer 拒絕回答

Q37. Right to data portability – the possible amendment is to give data subjects the right to direct data users to transmit their personal data to other data users in a structured, open and machine-readable format and the rationale is to enhance the flow of personal data among service providers and improve competition in the data economy

資料可攜權 - 有關修改可能是，賦予資料當事人有權指示資料使用者將其個人資料以有組織的、開放的和機器可讀的格式轉移至其他資料使用者，理由是可提升服務供應商之間的個人資料流通，以及增強在數據經濟下的競爭。

1. 0－10 0-10
2. No idea / don’t know 不知道
3. Refuse to answer 拒絕回答

Q38. Data user return scheme – the possible amendment is to repeal s.14 to s.17 of the PDPO relating to the requirements of data users to submit prescribed information (i.e. data user returns) to the PCPD and the rationale is that implementation of data user return scheme will create administrative and financial burdens to both data users and the PCPD which is disproportional to the expected benefits of the scheme.

資料使用者申報計劃 - 有關修改可能是，廢除《個人資料（私隱）條例》第 14 條至第 17 條關於要求資料使用者向個人資料私隱專員公署呈交訂明資訊 (即資料使用者申報)，理由是實施資料使用者申報計劃，會為資料使用者及個人資料私隱專員公署造成行政和財務負擔，這與有關計劃的預期效益不成比例。

1. 0－10 0-10
2. No idea / don’t know 不知道
3. Refuse to answer 拒絕回答

Thank you for answering the questions.

問卷已完成，謝謝。

End of Questionnaire

問卷完