41st International Conference of Data Protection and Privacy Commissioners

21-22 October, Tirana, Albania

ICDPPC Data Protection Metrics Working Group

Report to the 41st Conference on Common Core Survey Questions

September, 2019

Table of Contents

Introduction

The 38th Conference adopted the Resolution on Developing New Metrics of Data Protection encouraging the Conference to help to develop internationally comparable metrics in relation to data protection and privacy and to support the efforts of other international partners to make progress in this area.

A sub-working group explored the usefulness of adopting common questions to be included in public attitude surveys by Conference members. This contributed to the following aims of the resolution -

a. *encourage member authorities to include certain common core questions in their regular community attitude surveys touching upon for example awareness levels of DPAs and applicable privacy and data protection law;*
b. *Centrally receive the results, make them available and calculate benchmarks;*

The working group recommends the Conference endorse four questions in the core areas of:

- public awareness of privacy law and authorities,
- trust in public and private sectors, and
- knowledge of data protection and privacy rights,

A selection of common questions will give members the ability to choose the questions that complement and fit into their existing survey questionnaires.

Conference members would be asked to submit the results of any survey using the recommended questions to the Secretariat for the information of members and the development of benchmarks.

There is scope for the development of additional common questions, but further work would be required.

It must be noted that the Asia Pacific Privacy Authorities Forum in 2014 adopted a statement of common administrative practice on recommended common core questions for community attitude surveys. The system in place encourages their members to include two common questions where members authorities undertake community attitude surveys.

Recommendations

The ICDPPC Data Protection Metrics working group recommends that the Conference agree to:

1. endorse four questions in the core areas of public awareness privacy law and authorities, trust in public and private sectors, awareness of data protection and privacy rights, and

2. create an exclusive webpage on the Conference website as a resource on Data Protection Metrics which would serve as a repository of the results of surveys undertaken by Conference members and list all the community attitude surveys made available with this report.

Project on common core questions

In 2017 the working group identified a long list of 38 potential projects to meet the objectives of data protection metrics resolution. One such project that would directly implement the resolution is the common core questions project.

New Zealand offered to lead this work and assembled existing series of published privacy surveys and identified commonalities amongst the survey questions used.

The working group agreed that there was substantial value in developing common questions in core areas. We agreed that recommended questions should be:

- relatively few and capable of agreement and adoption by consensus by all, and
- limited to core areas (which we identified as including awareness levels of law and privacy enforcement authorities, and possibly also high-level attitudes to privacy).

The recommended questions should be adopted by way of a resolution put to the Conference.

To facilitate easy access to the surveys used in the review of this project, it is recommended the community attitude surveys to be published on the Conference website to create an online repository on the website and results of surveys undertaken by Conference members. New Zealand can assist the Secretariat in the creation of suitable content and location on the website.

Recommended questions

The recommended questions concern awareness levels of an

- jurisdiction's data protection or privacy law
- data protection or privacy authority, and
- data protection and privacy rights,

The working group considered these to be core areas and the four questions quite suitable for recommended use.

Topic	Question
Data protection or privacy law	Are you aware of the (name of the data protection or privacy law)?
Data protection or privacy authority	Are you aware of the (name of the data protection or privacy authority)?

Knowledge of data protection and privacy rights	Are you aware of your data protection and privacy rights?
Trust in public and private organisations	Do you trust public organisations with your personal information or data? Do you trust private organisations with your personal information or data?

Attachment 1: Common themes in survey questions

- Privacy Law awareness
- Trust in public bodies (government)
- Trust in private sector
- Social media
- Privacy enforcement authority
- Use of information
- Misuse of information
- Online harassment
- Cybercrime
- Data transfers
- Marketing
- Data breach
- Sharing of information
- Identity theft
- Surveillance
- Electronic records
- Storage of information
- Tech products
- Collection of information
- Internet
- Disclosure of information
- De-identification
- Forced consent
- Online behaviour
- Consent
- Re-identification
- Privacy polices
- Types of websites
- Information online
- Online security
- Biometric data
- Complaints body
- Intelligence and oversight agencies
- Awareness of access right
- Access to information from agencies
- Collection of information
- Correction of information
- Lost or stolen information
- Activities prohibited under privacy law
- Providing information
- Awareness of PEA tools and resources
- Awareness of PEA tools
- Sensitive data
- Attitudes about public access to information
- Knowledge of privacy rights
- Concerns about protecting privacy
- Information management
- Business behaviour towards privacy
- Government behaviour towards privacy
- Erosion of privacy
- Privacy invasion
- Identity theft
- Access of privacy and security related technologies
- Confidence in business
- Confidence in government
- Electronic health records
- Disclosure of health information
- Inappropriate access of information
- Managing complaints
- Use of APPs
- Changes to data protection law
- Awareness of privacy
- Security threats
- Privacy risks
- Credit information
- GDPR

Attachment 2: A selection of surveys on data protection and privacy

Albania

Information and Data Protection Commissioner

Survey: Privacy and safety of personal data of 15-18 years students on social networks

1. Which tool are you using to access internet?
2. Are you a user of social networks?
3. In which social network are you signed up?
4. How often do you update your social network?
5. How many friends do you have on your social network profile?
6. Which are the reasons of using a social network?
7. Do you know all your virtual friends?
8. Have you ever met a social network friend that you have never knew before?
9. Have you ever been a victim of insults and offensive comments?
10. Where do you address when encountering a problem?
11. Are you aware on privacy policies on the social network?
12. Do you think that privacy policies are clear enough to be understood?
13. Are you informed on the security measures in the social network you are using?
14. Do you know that you may submit a complaint to the Information and Data Protection Authority in case your right to protect personal data is violated?

Armenia

Personal Data Protection Agency

Survey: included in annual report (October 2015 – January 2016)

1. Are you aware that according to the RA Law on Personal Data Protection you have the right to know, demand and receive the information about you stored in the organisations (public and private)?
2. Are you concerned that the organisations (public and private) can keep your personal data? Please provide your reasons for your concern.
3. When you sign a contract or an agreement, for example with a bank or telecommunication company, do you get to know how they are going to use the data you transmitted to them?

Australia - Federal

Office of the Australian Information Commissioner

Survey: Australian Community Attitudes to Privacy Survey 2017

[Questions extracted from survey report]

Q1: I'd like to start by asking you what you think are the biggest privacy risks that face people today in Australia?

- Ways my personal information can be lost
- Online services too easily available/ accessible/ not secure
- Smart phones/ apps
- ID scanning
- How frequently we have to give out personal information
- Sending information overseas
- Criminal history too easy to access
- Risk to me or my information
- ID theft/ fraud
- Data security/ data breaches
- Financial details/ information/ fraud
- Unauthorised monitoring of information/ data mining
- Organisations misusing my personal information
- Government information sharing/ information collection
- Commercial interests/ marketing about buying habits/ profile
- Surveillance
- Unsolicited phone calls
- Workplace privacy
- Credit reporting
- Other
- Don't know

Q2: What types of information are you reluctant to provide?

- Financial status
- Contact information
- Address
- Phone number
- Name
- Email address
- Date of birth
- All personal information/ identification
- Photo ID/ passport/ driver's licence number/ cards
- Medical or health information
- How many people/ men/ women in the household
- Work status and related information
- Sexual orientation

- Religion
- Marital status
- Ethnicity
- Buying preferences/ spending habits
- Other
- None
- Don’t know
- Refused

Q3: And which one of these [list answers given for Q2] do you feel MOST reluctant to provide?

Q4: What is your MAIN reason for not wanting to provide [answer from Q3]?

Q6: Were you aware that an Australian Government Privacy Commissioner exists to uphold privacy laws and to investigate complaints concerning the misuse of personal information?

Q6B: Which of the following do you think are under the jurisdiction of the Privacy Act?

- Federal government agencies
- Medium to large Australian businesses
- Public schools and universities
- Businesses collecting work related information about employees
- State government agencies
- Media organisations
- Small Australian businesses
- Political parties and political representatives
- Multinational organisations operating in Australia

D6: How often do you buy products online?

- At least once a month
- Less often than once a month
- Never buy products online
- Don’t know

Q8: How trustworthy or untrustworthy would you say organisations are with regards to how they protect or use your personal information

Very trustworthy – somewhat trustworthy – neither – somewhat untrustworthy – very untrustworthy – don’t know

- Health service providers
- Financial institutions
- State government departments
- Federal government departments
- Insurance companies
- Charities
- Companies in general

- Organisations providing technology products
- Retailers
- Real estate agents
- Market and social research organisations
- Debt collectors
- eCommerce industry
- Social media industry

Q9/10/11: How likely or unlikely are you to provide your personal information to an organisation if it meant you would receive rewards and benefits/the chance to win a prize/better customer service?

- Very likely
- Somewhat likely
- Neither
- Somewhat unlikely
- Very unlikely
- Don't know

Q11B: How comfortable or uncomfortable would you be with the personal information that you've provided to government agencies and departments being used for research, service development or policy development purposes?

Q12: Which of the following instances would you regard to be a misuse of your personal information?

Q13: How concerned are you about organisations sending their customers' personal information from Australia to overseas?

- Not concerned
- Somewhat concerned
- Very concerned

Q14A/AA: If a government agency/business loses my personal information they should tell me

Q14B: How comfortable or uncomfortable are you about businesses sharing your personal information with other organisations?

- Very comfortable
- Somewhat comfortable
- Neither comfortable nor uncomfortable
- Somewhat uncomfortable
- Very uncomfortable
- Don't know

Q14C: And how comfortable or uncomfortable are you with government agencies sharing information with other government agencies?

Q15A: Are you aware that you can request to access your personal information from businesses and government agencies?

Q17: If you wanted to report misuse of your personal information to someone, who would you be MOST likely to contact?

Q18/19 Have you ever decided not to deal with a government agency/private company because of concerns over the protection or use of your personal information?

- Decided not to deal with because of privacy
- Have never boycotted because of privacy
- Don't know

Q21: In order to protect your personal information, do you…

Always – often – sometimes – rarely – never – don't know

- Check that a website is secure before providing personal information
- Shred documents
- Adjust privacy settings on a social networking website
- Clear your browsing and search history
- Choose not to use an app on a mobile device
- Ask public or private sector organisations why they need your information
- Read privacy policies and notifications before providing personal information
- Choose not to deal with an organisation because of concerns regarding privacy
- Refuse to provide personal information
- Provide false personal details

Q24: Thinking now about using the internet. What proportion of websites do you think collect information about the people who visit them? Would you say it is...

- Can't estimate
- None
- Few
- Some
- Most
- All

Q24A: Now thinking about your smartphone. What proportion of smart phone apps collect information about the people who use them? Do you think it is...

- All
- Most
- Some
- Few
- None
- Can't estimate

Q25A: As you may be aware, search engines and social networking sites track your internet use in order to do things like target advertising at you. How comfortable are you with... search engines and social media sites targeting advertising at you based on what you have said and done online?

- Very comfortable
- Somewhat comfortable
- Neither
- Somewhat uncomfortable
- Very uncomfortable
- Don't know

Q25B: As you may be aware, search engines and social networking sites track your internet use in order to do things like target advertising at you. How comfortable are you with… search engines and social media sites keeping databases of information on what you have said and done online?

- Very comfortable
- Somewhat comfortable
- Neither
- Somewhat uncomfortable
- Very uncomfortable
- Don't know

Q26: Have you ever put any information on a social networking site that you've later regretted sharing with others?

- Yes
- No
- Have never posted information on social networking site
- Don't know

Q27: Do you think that social networking is... mainly a private activity, where users share information with their friends or mainly a public activity where users publish information which can be seen by many people?

- Private
- Public
- Don't know

Q29: Are you more or less concerned about the privacy of your personal information while using the internet than you were five years ago?

- More
- Less
- Same
- Don't know

Q29A: Generally speaking, do you believe there are greater privacy risks when dealing with an organisation online compared to traditional settings like going into a branch or on paper?

- Yes, greater privacy risks online
- No, there are not greater privacy risks online
- Don't know

Q30: Do you normally read the privacy policy attached to any internet site?

- Yes
- No
- Don't know

Q31: What impact, if any, did seeing or reading these privacy policies have upon your attitude towards the site?

- Helps me decide whether to use the site or not
- Good idea/ approve of the privacy policy/ prefer to see/ respect sites for having
- Feel more confident/ comfortable/ secure about using site
- Appear more honest/ trustworthy/ responsible/ legitimate
- Still apprehensive about sites that have them/ don't trust them/not convinced
- Made me more cautious/ aware when using the internet generally
- Too long/ complicated to read – it didn't build any confidence in the site
- No real impact/ no change
- Other
- Don't know

Q33: Which of the following statements BEST DESCRIBES how you GENERALLY feel when organisations that you have NEVER DEALT WITH BEFORE send you unsolicited marketing information?

- Annoyed
- Concerned about where they obtained it
- It's a bit annoying but it's ahrmless
- It doesn't bother you
- You don't mind getting it at all
- Other
- Don't know

Q37: How concerned are you about using biometric information for you to…

Very concerned – somewhat concerned – not concerned – don't know

- Use tech devices (such as a smartphone or wearable device, such as a fitness tracker)
- Get into your place of work or study
- Go into a licensed pub, club, bar or hotel
- Do your day-to-day banking
- Get on a flight

Q38: Have you (or someone you personally know) ever been the victim of identity fraud or theft? (Multi response)

- Happened to me or someone I know
- Yes, it happened to me
- Yes, it happened to someone I personally know
- No
- Don’t know

Q39: How concerned are you that you may become a victim of identity fraud or theft in the next 12 months?

- Very concerned
- Somewhat concerned
- Not concerned
- Don’t know

Q40: I’d now like to ask you about credit ratings. Do you know what a credit rating is?

- Yes
- No
- Don’t know

Q41: Have you ever tried to get information about your credit rating? This is called your credit report.

- Yes
- No
- Don’t know

(Not all questions listed since survey report doesn’t display all the questions)

Australia (New South Wales)

Information and Privacy Commission

Survey 1: Attitudes of NSW Community to Privacy 2017

1. Which of the following activities do you believe are currently prohibited under the privacy legislation?
   - Government health records being made available to people other than those you provided it to e.g. another organisation
   - Photos of you being published on the internet without permission
   - Information about products and services that you use being disclosed to others without permission
   - Information about your family or social life being made public without permission
2. And which of them do you believe should be prohibited under the privacy legislation?
   - Government health records being made available to people other than those you provided it to e.g. another organisation
   - Photos of you being published on the internet without permission
   - Information about products and services that you use being disclosed to others without permission
   - Information about your family or social life being made public without permission
3. And which activity would you say is of most concern to you?
   - Government health records being made available to people other than those you provided it to e.g. another organisation
   - Photos of you being published on the internet without permission
   - Information about products and services that you use being disclosed to others without permission
   - Information about your family or social life being made public without permission
4. In general, are you more concerned about possible privacy breaches for yourself or for other family members such as your children?
   - More concerned for myself
   - More concerned for other family members, such as my children
   - Equally concerned for both
5. You said, information about your family or social life being made public without permission concerned you the most, why does that concern you?
   - Nobody's business but mine
   - The information could be used in ways that I don't know about
   - The information could be embarrassing or damaging
   - The information could be used in ways that put me at a disadvantage
   - It's not a good thing for our society as a whole
   - Other (please specify)
6. Do you believe that data collected about you can be fully de-identified, in the sense that your identity would not be apparent to anyone?
   - Yes
   - No
   - Not sure

7. I would now like to find out whether you would be prepared to have information about you disclosed for different purposes, assuming that the people using the information would be able to identify you.
   Firstly thinking about you or your family's health information. Would you agree or disagree with your information being used for each of the following purposes ..
   - To be used for research purposes
   - To help in planning and delivering government services
   - To help government agencies develop new policies
   - To help monitor the quality of government services
   - To monitor your use of articular products or services
   - As part of consulting with the public
8. I would now like to find out whether you would be prepared to have information about you disclosed for different purposes, assuming that the people using the information would be able to identify you.
   And what about your personal information such as name, address, date of birth, or images, would you agree or disagree with your information being used for each of these purposes
   - To be used for research purposes
   - To help in planning and delivering government services
   - To help government agencies develop new policies
   - To help monitor the quality of government services
   - To monitor your use of articular products or services
   - As part of consulting with the public
9. Do you believe that a government service provider should be able to make it a condition of obtaining the service that you must consent to the use of your health information to be used for purposes other than for the service you are seeking?
   - Yes
   - No
10. And what if it was your personal information that they could use for other purposes? Do you believe that a government service provider should be able to make it a condition of obtaining the service that they can use your personal information?
    - Yes
    - No
11. Would you agree to your health information being provided if you were told that this information could be 'fully de-identified'?
    - Yes
    - No
12. Would you agree if your health information was 'de-identified' and there was still a chance that you could be identified?
    - Yes
    - No
13. Would you agree to your personal information being provided outside of government if you were told that this information could be 'fully de-identified'?
    - Yes
    - No

14. Would you agree if your personal information was ‘de-identified’ and there was still a chance that you could be identified?
    - Yes
    - No
15. If you became aware that the information you had to provide when getting services could be make available to others, but you didn’t know who, and there was a chance that you may be able to be re-identified, what would you do?
    - Go elsewhere for the service if there was an alternative
    - Make a complaint
    - Go without the service(s)
    - Use the service but provide incomplete personal or health information
    - Depends NFI (no further information)
    - Use the service but provide inaccurate personal or health information
    - I would not worry
    - Get info/ ask for info about the process/ contact the authority concerned
    - Grumble/ freak out/ shriek
    - I would sue/ go into a class action suit
    - Other
16. If your privacy had been seriously breached by [breach] what do you think would be the ideal solution or course of action?
    Breach – a neighbour installing cameras that looked directly into your premises or someone was posting unwanted images of you online; An employee of the public sector releasing data to a non-government organisation without your consent; Internet service providers on-selling your information
    - Legal action
    - Financial compensation
    - Criminal offence
    - An order issued to require them to take the material down/ return it
    - An order issued to require them to apologise
17. How seriously do you think those in authority, including elected representatives, are taking privacy?
    - Very seriously
    - Quite seriously
    - Undecided
    - Not seriously at all
18. How often do you access social media?
    - Everyday
    - Every few days
    - Once a week
    - Once a fortnight
    - About once a month
    - Less often than once a month
    - Never
19. Which of these types of online media sources do you regularly use?
    - Facebook

- YouTube
- Smartphone apps
- Instagram
- Twitter
- Podcasts
- None of the above

Survey 2: IPC Omnibus 2014

1. Did you know, under NSW privacy law, that you have a right to access any personal information held about you by:
   - Public health service providers
   - Public education providers
   - Private health service providers
   - State governments departments
   - Local Councils
2. Do you know how to go about accessing this information? Yes/ No
3. What would you do to access it?
   - Google/ internet search
   - Phone the agency
   - Go to their website
   - See them in person
   - Make a written request
   - Email
   - Freedom of information laws
   - If unsuccessful, follow up with ombudsman/ advocate
   - Other
4. Have you ever considered accessing any personal information held about you by any of the following agencies?
   - State government departments
   - Public health service providers
   - Private health service providers
   - Public education providers
   - Local councils
5. Have you ever tried to access personal information held about you by any of the following agencies?
   - Public health service providers
   - Public education providers
   - State government departments
   - Private health service providers
   - Local councils
6. Were you successful in accessing your information from
   - Local councils
   - Public education providers
   - Private health service providers
   - Public health service providers
   - State government departments
7. If your personal information is held by an agency in NSW there are certain protections around it. Would you expect that it your personal information data went overseas or intestate that it would still have the same or similar privacy protections?
   - Yes / No / Don’t know

Bulgaria

Commission for Personal Data Protection

Survey: Data Protection Awareness Survey 2018

Part I: Standard questionnaire for data protection awareness evaluation

1. Are you aware that in May 2018 enters into force a new European Personal Data Protection Regulation?
2. Are you aware that the new European Regulation revokes the personal data controllers' obligation to register in CPDP?
3. Do you know that some controllers will have to appoint data protection officer?
4. Do you know which controllers will be obliged to appoint data protection officer under GDPR?
   - state or local authority
   - all private companies
   - only banks, mobile operators and insurance companies
   - all controllers, which activities require regular and systematic large scale surveillance of data subjects
   - controllers, which main activities consist in processing on a large scale of special categories of data and of personal data relating to criminal convictions and offences
   - only the controllers pointed out by CPDP
5. Are you aware that after entering into force of the GDPR the companies with more than 250 employed persons should maintain register for personal data processing?
6. Do you know what types of measures should the companies undertake by the personal data processing, in order to be compliant with the GDPR's audit obligation?
7. Do you know that the companies processing personal data should implement risk assessment procedure and do you plan measures?
8. Are you informed that everyone has "the right to be forgotten", e.t. to seize the collection and processing of his/her personal data?
9. Point out two rights which every personal data subject has according to the new GDPR:
   - correction, if data are incorrect or incomplete
   - to restrict the processing of his/her personal data by state authorities
   - data portability
   - to object to ungrounded personal data processing
   - to not submit personal data to anyone
   - to access to his/her personal data
10. Do you have trust in CPDP?
11. Have you ever exercised your personal data protection rights and are satisfied?
12. Would you send a complaint in CPDP, if with your personal data has been misused?
13. Do you think that there are sensitive data, which are not sufficiently protected?
    - political believes and preferences
    - customers preferences with regard to goods, fashion and other
    - others
    - no
    - don't know

Canada – Federal

Office of the Privacy Commissioner of Canada

Survey: 2016 Survey of Canadians on Privacy

1. How would you rate your knowledge of your privacy rights? Please use a scale of 1 to 7, where 1 means very poor and 7 means very good.
2. In general how concerned are you about the protection of your privacy? Please use a scale of 1 to 7, where 1 means not concerned at all, and 7 means extremely concerned.
3. Please rate the extent to which you agree or disagree with the following statements, using a scale of 1 to 7, where 1 means strongly disagree, and 7 means strongly agree.
   - I feel I have less protection of my personal information in my daily life than I did 10 years ago.
   - I feel confident that I have enough information to know how new technologies might affect my personal privacy.
   - I feel I can control how my personal information is collected and used by organisations.
4. Do you use the internet? And what about a mobile device, such as a smart phone or tablet?
   - Yes
   - No
5. When you think about the information available about you online, please tell me how concerned you are about each of the following? How about
   - Marketing companies using this information to analyse your likes and dislikes
   - Companies or organisations using this information to determine your suitability for a job or promotion
   - Companies or organisations using this information to make decision about you, such as for an insurance claim or health coverage

   Please use a 7 point scale, where 1 means not concerned at all and 7 means extremely concerned.
6. Some companies use information collected from an individual's internet browsing to present online ads tailored to that individual. Using a 7 point scale where 1 means strongly disagree and 7 means strongly agree, please rate the extent to which you agree or disagree with the following statements about targeted online ads:
   - Targeted online ads make me feel like I have less privacy online
   - I think websites should as for my consent before using information about my internet browsing activities for targeted online advertising
7. Please tell me if you do any of the following. Do you
   - Adjust settings on your smartphone or tablet to limit the amount of personal information that you share with others
   - Read the privacy policy for apps before you download them
   - Not install or uninstall apps if you are concerned about the personal information you are asked to provide?

8. Have you ever had anything posted online about you that negatively affected your life in some way? This could be something you posted yourself or someone else posted about you, and it could be a picture or words, or any other type of online posting.
   - Yes
   - No
9. Advances in technology are making it easier to collect and use information about our bodies, like our fingerprints and DNA, for non-medical purposes. Thinking about risks to personal privacy, how concerned would you be about providing information about your body in the following scenarios
   - Having your iris scanned in order to speed up border crossings into Canada and the United States
   - Providing a sample of your saliva to a company to perform genetic testing to help you learn more about your ancestry
   - Providing a sample of your saliva to a company to perform genetic testing to determine your likelihood for developing future health conditions
   - Allowing information about the number of steps you've taken, calories burnt and heart rate to be collected by a fitness tracker, analysed and used to make you commercial offers.

     Please use a 7 point scale where 1 means not concerned at all and 7 means extremely concerned.
10. Recently there have been a number of incidents reported in the news of sensitive personal information such as private photos and debit or credit information, being lost, stolen or made public. To what extent has this affected your willingness to share personal information with organisations? Please use a 7 point scale, where 1 is not at all and 7 is a great deal.
11. Have you ever
    - Refused to provide an organisation with your personal information? Yes/ No
    - Chosen to not do business with a company due to its privacy practices? Yes/ No
12. Many companies are collecting personal information about consumers to learn more about them. What impact would the following have on your willingness to do business with a company that collects your personal information? What if
    - The company provides clear, easy to understand information about its privacy practices, including how it uses personal information
    - The company provides a menu of options you would choose from to determine how, if at all, the company could use your personal information
    - The company's privacy practices are backed by a seal of approval provided by an independent authority on privacy protection
    - Under Canadian law, the company would fact strict financial penalties, such as large fines, for misusing your personal information.

    Would this definitely, probably, probably not, or definitely not increase your willingness to do business with the company?
13. Please rate the extent to which you agree or disagree with the following statements, using a 7 point scale where 1 means strongly disagree and 7 means strongly agree.

- Intelligence gathering and law enforcement agencies do not have enough power to collect private information from citizens in support of national security and public safety
- I don't have a good understanding of what the government of Canada does with the personal information it collects from citizens
- Intelligence gathering and law enforcement agencies should be required to publicly report on how often they make requests, without court authorisation, to receive information about individuals' online and telephone activities

14. How much do you understand about what information is collected, used, or disclosed by intelligence gathering activities in Canada? Would you say – a great deal, a moderate amount, not much, nothing at all?
15. The laws that govern the privacy obligations of federal departments and agencies were put in place for 30 years ago. Parliament is currently studying the law and determining how it may be updated. When modernising Canada's privacy laws would you say the government should definitely, probably, probably not, or definitely not
    - Prohibit government from collecting personal information about Canadians unless it is essential to administer a government program
    - Legally require government to consider the privacy risks of any new programs or laws
    - Legally require that the offices of Cabinet Ministers and the Prime Minister be subject to the same privacy law obligations that apply to government departments and agencies
    - Legally require government departments and agencies to put in place sufficient safeguards to protect the personal information they collect about Canadians
    - Legally require government to put recommendations in place to improve privacy protection practices following an investigation that identifies problems
16. How concerned you are personally using a scale of 1 to 7, where 1 means not at all concerned and 7 means extremely concerned
    - Government monitoring of your activities for national security or public safety purposes
    - The potential for things like photos or posts living forever on the internet and potentially harming your reputation
    - Your ability to get clear information from businesses enabling you to make informed choices about how they collect and use your personal information
    - The collection and use of information from your body like fingerprints, DNA, or fitness levels for non-medical reasons, such as determining eligibility and rates for insurance

Canada (Alberta)

Office of the Information and Privacy Commissioner

Survey: General Population Survey 2017

Section1: Awareness of access and privacy laws

1. Are you aware of any laws that are intended to protect your personal information or health information? (interviewer note: by personal information we mean things like name, address, date of birth, social insurance number, education, employment history, financial information, images of you)
   - Yes
   - No
   - Don't know
2. Which laws have you heard of?
   - Freedom of information and protection of privacy act
   - Health information act
   - Personal information protection act
   - Personal information protection and electronic documents act
   - Other (specify)
   - Don't know
3. Are you aware of any laws that are intended to provide individuals with the right to access their own personal or health information or government information?
   - Yes
   - No
   - Don't know
4. Which laws have you heard of?
   - Freedom of information and protection of privacy act
   - Health information act
   - Personal information protection act
   - Personal information protection and electronic documents act
   - Other (specify)
   - Don't know
5. Which of the following laws have you heard of?
   Yes aware – No unaware – Don't know
   - Freedom of information and protection of privacy act
   - Health information act
   - Personal information protection act
   - Personal information protection and electronic documents act
6. Please indicate if you are aware of the following
   Yes aware – No unaware – Don't know
   - You have the right to request access to general information held by public-sector bodies, such as government ministries, municipalities, universities and law enforcement agencies
   - You have the right to request access to your personal information or health information held by a public sector body, private business or health care provide

- You have the right to ask that errors in your personal information or health information be corrected
- When your personal information or health information is being collected from you, you have the right to be informed of the purposes for the collection

7. Thinking about your familiarity with Alberta's access to information and privacy laws, overall, would you say that you are
   - Not at all familiar
   - Somewhat familiar
   - Very familiar
   - Don't know

Section 2: Awareness of OIPC

8. Have you heard about the Office of the Information and Privacy Commissioner of Alberta before today?
   - Yes, aware
   - No, unaware
   - Don't know
9. How have you heard about the Commissioner's Office?
   - Television
   - Radio
   - The OIPC website
   - Online; non-OIPC website
   - Twitter
   - Publications or articles
   - Conferences
   - Through work/my job
   - Personal experience/have contacted the OIPC previously
   - Other (Specify)
   - Don't know
10. Regarding the Commissioner's Office, were you aware of the following?
    - Yes, aware
    - No, unaware
    - Don't know

A. You can file a complaint with the Commissioner's Office if you feel that your personal or health information has been improperly collected, used or disclosed by a public-sector body, health care provider or private business
B. You can ask the Commissioner's Office to review the response you received from a public-sector body, health care provider or private business regarding your request for access to information
C. The Commissioner's Office is separate from the Government of Alberta and reports directly to the Legislative Assembly

11. And how comfortable are you with your current knowledge and understanding of the Information and Privacy Commissioner's Office? Do you…?
    - Wish you were more informed about the Commissioner's Office

- Feel comfortable with your current level of knowledge and understanding
- Don't know

Section 3: OIPC Communications

12. If you needed to obtain information about your access to information and privacy rights under Alberta's laws, do you feel you would know where to look?
    - Yes
    - No
    - Don't know
13. Were you aware that the Commissioner's Office has information and tools available to the public to help them understand their access to information and privacy rights?
    - Yes
    - No
    - Don't know
14. Have you ever used any of these resources
    - Yes
    - No
    - Don't know
15. What were these resources?
    - Online/Website
    - Contacted the OIPC office
    - Public presentations or forums
    - Publications
    - Other (specify)
    - Don't know
16. Using a scale of 1 to 5, where 1 means "not at all effective" and 5 means "very effective", how effective would the following ways be for the Information and Privacy Commissioner's Office to provide you with information?
    - The Commissioner's office website
    - Blog
    - Facebook page
    - Twitter feed
    - YouTube
    - Newspapers, TV, Radio coverage
    - Public presentations or forums
    - Brochures/Pamphlets in public buildings
    - A helpdesk telephone number Albertans can call
17. Are there any other effective ways the Commissioner's Office could provide information to you?
    - Yes
    - None, no other ways possible
    - Don't know

Section 4: Trends and issues

18. In this section of the survey, we would like to discuss specific trends and issues concerning access to information and privacy. Using a scale of 1 to 5, where 1 means “not at all important” and 5 means “very important”, please rate the level of importance you place on access to information or privacy issues related to the following
    - Data migration (e.g. transferring your data between vendors or cloud service providers or transferring your data to service providers outside Canada)
    - Open Government (e.g. proactive disclosure, routine release of information)
    - Personal information sharing among public bodies, health care providers and private businesses
    - Access to personal/health information for research purposes
    - Businesses or governments using social media to communicate with you
    - Using your employer’s equipment and technology (e.g. computer) for your personal use
    - Businesses or governments collecting and using personal information from social media (e.g. background checks)
    - Use of personal mobile devices at work (e.g. using your own cell phone for both personal and business purposes)
    - “Big Data” (i.e. businesses and governments collecting, compiling and analyzing vast amounts of personal information)
    - Children and youth privacy
    - Genetic information
    - Biometric identification (e.g. facial recognition, fingerprint, iris scans, etc.)
    - Surveillance (e.g. video surveillance, surveillance of Internet use, etc.)
    - Mobile device security
    - New technology (e.g. artificial intelligence, location tracking)
    - Identity theft/fraud
    - Hacking, malware, ransomware, email phishing
    - Mobile apps or wearable devices that collect personal or health information
    - Vehicles collecting data on driving habits
    - Direct access to your own records via internet portals, mobile apps, etc.
    - Inappropriate access by employees into records containing personal or health information
    - Government requiring businesses to collect and/or provide personal/health information to government
    - Online behavioural targeting and/or marketing
    - Identity management (e.g. management of individual identifiers, their authentication, authorization, and privileges and/or permissions within or across an electronic system)
19. Are there any other access to information or privacy related issues that you feel are important to Albertans?
    - Yes – specify
    - No
20. Using a scale of 1 to 5, where 1 means “strongly disagree” and 5 means “strongly agree”, please rate your level of agreement with the following statements
    - It is important to protect the right to access information in Alberta

- I am confident about my ability to access information
- It is important to protect the privacy of personal and health information
- I feel secure about the privacy of my own personal and health information
- I feel more secure about the privacy of my own personal and health information than I did five years ago

Canada (British Columbia)

Office of the Information & Privacy Commissioner

Survey: Public Awareness Survey

1. Have you heard of the OIPC?
   - Yes, aware
   - No, not aware
2. Of the people who have heard of the OIPC would you wish to be more informed about the Commissioner's office
   - Yes
   - No
3. Awareness of the functions of the OIPC –
   - You can file a complaint with the Commissioner's Office if you feel that your personal or health information has been improperly collected, used or disclosed by a public sector body, health care provider or private business
   - You can ask the Commissioner's Office to review the response you received from a public sector body, healthcare provider or private business regarding your request for access to information
   - The Commissioner's Office is separate from the Government of BC and reports directly to the legislative assembly

     Yes, aware – No, not aware
4. Are you familiar with BC's access to information and privacy laws
   - Very familiar
   - Somewhat familiar
   - Not familiar
5. Are you aware of the following laws
   - FIPPA/ FOIPPA
   - PIPA

     Yes, aware – No, not aware
6. Awareness of privacy rights: did you know
   - You have the right to ask that errors in your personal information or health information be corrected
   - When your personal information or health information is being collected from you, you have the right to be informed of the purposed for collection
   - You have the right to request access to your personal information or health information held by a public-sector body, private business or healthcare provider
   - You have the right to request access to general information held by public sector bodies such as government ministries municipalities, universities and law enforcement agencies

     Yes, aware

     No, not aware
7. Have you ever refused to provide an organisation with your personal information?
   - Yes, have refused
   - No, have not

- Can’t recall

8. In the past year, have you asked a company how it uses your personal information or protects your privacy
   - Yes, have asked
   - No, have not
   - Can’t recall
9. On a scale of 1 to 7 where 1 – 3 is not affected and 6-7 is affected a great deal, how affected will you be if your personal information is lost, stolen or made public on willingness to share personal information

Perceptions of businesses and government

10. How seriously do you think businesses take their responsibility to protect personal information
    - Not seriously
    - Somewhat seriously
    - Very seriously
11. How seriously do you think the provincial government takes their responsibility to protect personal information
    - Not seriously
    - Somewhat seriously
    - Very seriously

Attitudes regarding public access to information

12. Please indicate if you agree, somewhat agree or disagree with the following
    - The public has a fundamental right to access government information
    - Public access to government information is critical to a well-functioning democracy
    - Public access to government information ensures government is accountable
    - Government should be taking steps to make as much information as possible easily accessible to the public
    - Public access to government information ensures the public is able to judge the performance of the government fairly

Canada (Manitoba)

Office of the Manitoba Ombudsman

Survey: Privacy and Security: A Manitoba Perspective

Erosion of personal privacy

1. I feel I have less personal privacy in my daily life than I did five years ago
   - Disagree
   - Neither
   - Agree

Concern about erosion of privacy

2. I am concerned about how my privacy is being eroded
   - Disagree
   - Neither
   - Agree

Privacy invasions

3. Have you ever experienced a serious invasion of privacy?
   - Yes
   - No

Threat of privacy invasion

4. How likely is it you will experience a serious invasion of your personal privacy over the next two years?
   - Don't know
   - Not at all likely
   - Slightly likely
   - Somewhat likely
   - Very likely
   - Extremely likely

Victims of identity theft

5. Have you ever been a victim of identity theft? By identity theft, we mean the unauthorized collection and fraudulent use of someone else's personal information, usually for criminal purposes.
   - Yes
   - No
   - Don't know

Extent of perceived threat posed by identity theft

6. How serious a problem is identity theft in Canada today?
   - Don't know
   - Not at all likely
   - Slightly likely
   - Somewhat likely
   - Very likely

- Extremely likely

Level of concern regarding identity theft

7. How concerned are you personally about being a victim of identity theft?
   - Don't know
   - Not at all likely
   - Slightly likely
   - Somewhat likely
   - Very likely
   - Extremely likely

Submitting personal information online

8. In the past year, have you submitted personal information such as your credit card number, name, address, your income over the internet? What types of personal information have you submitted over the internet in the past year?

Awareness of privacy and security related technologies

9. To what extent are you aware of the following products, services and new technologies?
   Not at all likely - Slightly likely - Somewhat likely - Very likely - Extremely likely
   - Encryption
   - Cookies
   - Public key infrastructure

Actions taken when information is requested

10. How often have you done the following in the past year?
    Not in past year – rarely – sometimes – regularly
    - Refused to provide information to businesses when you felt it is either too personal or not necessary
    - Asked a business why they are asking for certain information
    - Deliberately provided incorrect information to a store or company that asked for personal information

Attempted to remove name from marketing lists

11. How often have you attempted to take your name off marketing lists in the past year?
    - Not in part year
    - Rarely
    - Sometimes
    - Regularly

Actions taken online to protect information

12. How often have you done the following in the year
    Not in past year – rarely – sometimes – regularly
    - Read a company's privacy policy on their website
    - Use secondary email accounts to keep your identity better protected while on the internet

Household document shredder ownership

13. Do you or anyone in your household have a personal shredder used to destroy documents such as credit card statements or other type of personal documents?
    - Yes
    - No

Lodged a complaint about how information used

14. Have you lodged a complaint if you were unhappy with how an organisation handled your information in the past year?
    - Yes
    - No

Request to see information kept by organisations

15. Have you requested to see personal information about yourself that is kept by government in the past year?
    - Yes
    - No
16. Have you requested to see personal information about yourself that is kept by a business in the past year?
    - Yes
    - No

Individual responsibility

17. It's up to individuals to protect their own personal privacy
    - Disagree
    - Neither
    - Agree

Awareness of who to turn to if invasion experienced

18. I have a good idea of who to turn to if I ever experience an invasion of my privacy?
    - Disagree
    - Neither
    - Agree

Organisation turned to if invasion experienced

19. If you were to experience a serious invasion of privacy, who would you be most likely to turn to?
    - The police
    - Depends on situation
    - Family member/friends
    - Lawyer
    - Source of invasion (e.g. offending company)
    - Member of parliament
    - Federal government
    - Provincial government
    - Federal/Provincial privacy Commissioner
    - Consumer advocate

- Other
- Don’t know

Familiarity with privacy laws

20. How familiar are you with federal and provincial privacy laws that place restrictions on how governments and businesses can use Canadians’ personal information?
    - Not at all familiar
    - Slightly familiar
    - Somewhat familiar
    - Very familiar
    - Extremely familiar

Confidence privacy laws will be adhered to

21. How much confidence do you have that federal government departments and provincial government ministries will follow their own privacy laws regarding usages of Canadians’ personal information?
    - Don’t know
    - Not at all confident
    - Slightly confident
    - Somewhat confident
    - Very confident
    - Extremely confident
22. How much confidence do you have that businesses will follow federal and provincial government privacy laws regarding usages of Canadians’ personal information?
    - Don’t know
    - Not at all confident
    - Slightly confident
    - Somewhat confident
    - Very confident
    - Extremely confident

Implications for misuse of personal information by financial institutions

23. I wouldn’t hesitate to switch financial institutions if I felt they were using my personal information in ways that I didn’t consent to
    - Disagree
    - Neither
    - Agree

Control of personal information held by governments

24. I have control over how my personal information is being used by governments.
    - Disagree
    - Neither
    - Agree

Perception of government information collection

25. Which of the following statements is closer to your point of view?

- Governments collect only the personal information they need to when they provide services to Canadians
- Governments collect far more personal information than they actually need to when they provide services to Canadians
- Don't know

Perception of government information management

26. The federal government has one large database on me with all my personal information on it
    - Don't know
    - Disagree
    - Neither
    - Agree
27. My provincial government has one large database on me with all my personal information in it
    - Don't know
    - Disagree
    - Neither
    - Agree

Perceived government access to personal information

28. There is no real privacy because the government can learn anything they want about you
    - Disagree
    - Neither
    - Agree

Broad trust in government

29. Governments can be trusted to do the right thing
    - Disagree
    - Neither
    - Agree

Internet use and GOL uptake

30. In the past 3 months, have you used the Internet, either at home or elsewhere?
31. Have you (has anybody) ever done any of the following activities with governments over the internet (on your behalf)?
    - Visited a government website
    - Downloaded a government form
    - Submitted income taxes
    - Sent an email to a government employee
    - Made a payment
    - Sent an email to a Canadian politician
    - Applied for a program
    - None of the above

Comfort with Electronic Health Record

32. Overall, how comfortable are you with a system where your health information is stored electronically in this way?
    - Don’t know
    - Not at all comfortable
    - Slightly comfortable
    - Very comfortable
    - Extremely comfortable

Privacy concerns and health-care

33. In the past year, have you withheld information from a health-care provider because of concerns over who it might be shared with or how it might be used
    - Yes
    - No
34. In the past year, have you decided not to see a health-care provider because of concerns over who your health information might be shared with or how it might be used
    - Yes
    - No

Canada (Saskatchewan)

Office of the Saskatchewan Information and Privacy Commissioner

Survey: Privacy and Access to Information Survey

Seeking out information

1. Have you ever actively sought out information about your privacy or access to information rights?
2. (responses that said yes to Q4) What did you do first to find this information?
    - Typed your privacy-related query into a search engine
    - Searched specifically for the website of the office of the Saskatchewan information and privacy commissioner
    - Consulted social media
    - Searched specifically for the website of the office of the privacy commissioner of Canada
    - Contacted a government office or agency (federal, provincial, municipal)
    - Consulted print media, such as books, newspapers or magazines
    - Directly contacted the office of the Saskatchewan information and privacy commissioner
3. (responses that said no to Q4) If you need to find this information what would you do first?
    - Type your privacy related query into a search engine(i.e. “google it”)
    - Search specifically for the website of the Office of the Privacy Commissioner of Canada
    - Contact a government office or agency (federal, provincial, municipal)
    - Directly contact the office of the privacy commissioner of Canada
    - Consult social media
    - Consult print media, such as books, newspapers or magazines
    - Directly contact the office of the Saskatchewan information and privacy commissioner

Awareness and familiarity with privacy laws and acts

4. Thinking about your familiarity with SK’s access to information and privacy laws
    - Very familiar with these laws
    - Somewhat familiar with these laws
    - Not familiar with these laws
5. Are you aware of the Freedom of Information and Protection of Privacy Act
    - Very familiar
    - Somewhat familiar
    - Not familiar
6. Are you aware of the Health Information Protection Act
    - Very familiar
    - Somewhat familiar

- Not familiar

Awareness of privacy rights

7. Please indicate if you are aware of the following
   Yes, aware of this privacy right – no, not aware of this privacy right
   - You have the right to ask that errors in your personal information or health information be corrected
   - You have the right to request access to your personal information or health information held by a public –sector body, private business or healthcare provider
   - When your personal information or health information is being collected from you, you have the right to be informed of the purposes for collection
   - You have the right to request access to general information held by public bodies such as government ministries, municipalities, universities and law enforcement agencies

Awareness of the office of the Information and Privacy Commissioner

8. Before today, had you heard of the Office of the Saskatchewan information and privacy commissioner?
   - Yes
   - No
9. Regarding the information and privacy commissioner's office were you aware of the following?
   Yes, aware – No, not aware
   - You can file a complaint with the Commissioner's Office if you feel that your personal or health information has been improperly collected, used, or disclosed by a public sector body, health care provider or private business
   - You can ask the Commissioner's Office to review the response you received from a public sector body, healthcare provider or private business regarding your request for access to information
   - The Commissioner's office is separate from the Government of SK and reports directly to the Legislative Assembly
10. How comfortable are you with your current knowledge and understanding of the Information and Privacy Commissioner's Office?

Perceptions of businesses and government

11. In your opinion, how seriously do businesses take their responsibility to protect consumer personal information? Please use a scale from 1 to 7, where 1 means not at all seriously and 7 means extremely seriously.
12. In your opinion, how seriously do the provincial government take their responsibility to protect consumer personal information? Please use a scale from 1 to 7, where 1 means not at all seriously and 7 means extremely seriously.

Impact of mishandling of personal information

13. Recently there have been a number of incidents reported in the news of employees snooping into patients' medical and other records. To what extend has this affected your willingness to share personal information with organisations? Please use a scale of 1 to 7, where 1 is not at all and 7 is a great deal.
14. Have you ever refused to provide an organisation with your personal information?
    - Yes, have refused
    - No, have not
    - Can's recall
15. In the past year, have you asked a company how it uses your personal information or protects your privacy
    - Yes, have asked
    - No, have not
    - Can't recall
16. On a scale of 1 to 7 where 1 – 3 is not affected and 6-7 is affected a great deal, how affected will the public's willingness to share personal information be if your sensitive personal information is being accessed inappropriately.

Impact of company privacy practices and reputation

17. Would you choose to do business with a company specifically because it
    Yes - No
    a. Does not collect your personal information
    b. Has a good reputation for its privacy practices

Attitudes regarding public access to information

18. On a scale of 1 to 7, where 1 to 3 is disagree, 4 to 5 is somewhat agree and 6 to 7 is strongly agree do you think
    - The public has a fundamental right to access government information
    - Public access to government information is critical to a well-functioning democracy
    - Public access to government information ensures government is accountable
    - Government should be taking steps to make as much information as possible easily accessible to the public
    - Public access to government information ensures the public is able to judge the performance of the government fairly
19. On a scale of 1 to 7, where 1 to 3 is disagree, 4 to 5 is somewhat agree and 6 to 7 is strongly agree do you think
    - I feel I have less protection of my personal information in my daily life than I did 10 years ago
    - I have little expectation of privacy today, either online or in the real world, because there are so many things that can compromise it
    - I am satisfied with the current level of public access to government information
    - I feel confident that I enough information to know how new technologies might affect my personal privacy
    - I feel confident that when I share my personal information with an organisation, I understand how it will be used

- I have been negatively affected as a result of an organisation misusing, sharing or losing my personal information

Hong Kong

Survey: Baseline survey of public attitudes on privacy and data protection 2014

1. How much do you mind if your ID card details are noted down by a police officer when he stops you in the street?
   - 0-10
   - No idea
   - Refuse to answer
2. How much do you mind if your name and ID card number are noted down by a security guard in order to let you into a residential building as a visitor?
   - 0-10
   - No idea
   - Refuse to answer
3. How much do you mind providing your ID card number to postman when collecting parcels?
   - 0-10
   - No idea
   - Refuse to answer
4. How much do you mind providing your ID card copy when attending a job interview, after shortlisting, but before receiving a job offer?
   - 0-10
   - No idea
   - Refuse to answer
5. How much do you mind providing your ID card number when enrolling for fitness club membership?
   - 0-10
   - No idea
   - Refuse to answer
6. How much do you mind providing a copy of your ID card when enrolling for fitness club membership?
   - 0-10
   - No idea
   - Refuse to answer
7. How much do your mind providing a copy of your ID card when enrolling for fitness club membership?
   - 0-10
   - No idea
   - Refuse to answer

Now I'll ask you similar questions about how much you mind providing different types of personal data in return for a discount card from a retail shop where you frequently buy things, on the 0-10 scale where 0 means you do not mind at all and 10 means you would certainly refuse.

8. Your full residential address?
    - 0-10
    - No idea
    - Refuse to answer
9. Your mobile phone number?
    - 0-10
    - No idea
    - Refuse to answer
10. Your ID card number?
    - 0-10
    - No idea
    - Refuse to answer
11. Your personal income?
    - 0-10
    - No idea
    - Refuse to answer
12. Your occupation?
    - 0-10
    - No idea
    - Refuse to answer
13. Your date, month and year of birth?
    - 0-10
    - No idea
    - Refuse to answer

I am going to list some situations, which may be an invasion of personal data privacy. Please use a number between 0 and 10 where 0 means it is not an invasion of personal data privacy and 10 is a very severe invasion of personal data privacy.

14. Marriage registry exhibits the ‘notice of intended marriage’ containing the occupation of the intended marrying parties in places open to public for 3 months.
    - 0- 10
    - Difficult to say/ no idea/ don’t know
    - Refuse to answer
15. Name of registered owners and the value of the property transaction can be checked out by anyone in the Lands Registry.
    - 0- 10
    - Difficult to say/ no idea/ don’t know
    - Refuse to answer
16. Full HKID card number of a company director can be checked out by anyone in the Companies Registry.
    - 0- 10
    - Difficult to say/ no idea/ don’t know
    - Refuse to answer

17. Residential address of a company director can be checked out by anyone in the Companies registry
    - 0- 10
    - Difficult to say/ no idea/ don't know
    - Refuse to answer
18. CCTV covering the doorway of your flat.
    - 0- 10
    - No idea/ don't know
    - Refuse to answer
19. Your friends/ relatives refer you to a retail shop and provide your name and address to the retail shop when he/she applies for a loyalty card without getting your agreement first.
    - 0- 10
    - No idea/ don't know
    - Refuse to answer
20. You refer your friends/ relatives to a retail shop and provide their names and addresses in the application form for a loyalty card without getting their agreement first
    - 0- 10
    - No idea/ don't know
    - Refuse to answer

Misuse of personal data

21. Have you personally experienced what you consider to be a misuse of your personal data within the last 12 months? (If yes, ask Q22,otherwise, skip to Q25)
    - Yes
    - No (skip to Q25)
    - Difficult to say/ no opinion/ can't remember/ don't know (skip to Q25)
    - Refuse to answer (skip to Q25)
22. Who or what type of organisation was responsible for the last misuse of your personal data?
    - Government departments
    - Banks
    - Money lending companies
    - Public hospitals
    - Private hospitals
    - Insurance companies
    - Real estate agents
    - Property management
    - Schools
    - Telecommunications companies
    - Social services organisations
    - Mass media/ journalists
    - Fitness and beauty centres
    - Retails outlets

- Your employer
- Family members living in the same household
- Friends/ classmates/ colleagues
- Neighbours
- Other individuals
- Other organisations
- Difficult to say/ no opinion/ can't remember/ don't know
- Refuse to answer

23. Did you make a complaint about this case of your personal data being misused?
    - Yes (skip to Q25)
    - No
    - Difficult to say/ no opinion/ don't know
    - Refuse to answer (skip to Q25)
24. What is your main reason for not lodging a complaint?
    - Cannot afford the time
    - Not worthwhile
    - Troublesome
    - Don't know where to lodge a complaint
    - Did not know the right conferred by the law
    - Other reasons, please specify
    - Difficult to say/ no opinion/ don't know
    - Refuse to answer

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

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

25. Mass media (e.g. news on TV, newspaper and radio or advertisements)
    - Yes
    - No
    - No idea
    - Refuse to answer
26. PCPD's publications (e.g. guidance notes, pamphlets, fact sheets and code of practices)
    - Yes
    - No
    - No idea
    - Refuse to answer
27. PCPD website and multimedia (e.g. web videos)
    - Yes
    - No
    - No idea
    - Refuse to answer
28. PCPD publicity programmes (e.g. seminars, workshops and exhibitions)

- Yes
- No
- No idea
- Refuse to answer

29. In 2010, Octopus admitted to sharing personal data with five business partners without providing adequate notice to consumers and obtaining customer's consent.

    To what extent do you agree that the PCPD has increased community awareness of personal data privacy issues after the Octopus Incident in 2010? Do you strongly agree, agree, disagree or strongly disagree?
    - Strongly agree
    - Agree
    - Disagree
    - Strongly disagree
    - Difficult to say/ no opinion/ don't know
    - Refuse to answer

What is your opinion on the trustworthiness of the following organisations when handling complaints? Please tell me a number indicating the level of trustworthiness, 0 means that you have no trust and 10 means total trust.

30. Consumer council
    - 0-10
    - Difficult to say
    - No idea/ don't know
    - Refuse to answer
31. Hong Kong Police Force
    - 0-10
    - Difficult to say
    - No idea/ don't know
    - Refuse to answer
32. The Ombudsman Hong Kong
    - 0-10
    - Difficult to say
    - No idea/ don't know
    - Refuse to answer
33. Equal Opportunities Commission
    - 0-10
    - Difficult to say
    - No idea/ don't know
    - Refuse to answer
34. Independent Commission against Corruption
    - 0-10
    - Difficult to say
    - No idea/ don't know

- Refuse to answer

35. Office of the Privacy Commissioner for Personal Data
    - 0-10
    - Difficult to say
    - No idea/ don't know
    - Refuse to answer

Privacy/ security concerns about transactions on the Internet

36. Google currently offers internet search and basic email services for free in return for showing you advertising which is targeted based on the information Google collected and analysed from your previous search and email behaviour. If Google was to offer comparable services of search and email, but without any advertising at all, how willing would you be to pay HK$20 per month for this, on a scale from 0-10 where 0 means I certainly would not use it and 10 means I certainly would be willing to pay this amount.
    - 0-10
    - Never use internet or email service
    - Difficult to say/ no opinion/ don't know
    - Refuse to answer
37. How often do you normally use Facebook?
    - Ever registered Facebook account but no longer use
    - Rarely
    - Less than weekly
    - At least weekly but less than daily
    - At least daily
    - No Facebook account (skip to Q41)
38. Are you aware that there are privacy settings in Facebook?
    - Yes
    - No (skip Q41)
    - Refuse to answer
39. Have you ever checked the privacy settings in Facebook?
    - Yes
    - No (skip to Q41)
    - Refuse to answer
40. Have you ever changed the privacy settings in Facebook?
    - Yes
    - No
    - Refuse to answer
41. Do you use a smartphone at all (i.e. phone with Internet access and apps)?
    - Yes
    - No
    - No idea
    - Refuse to answer

    If yes to Q42, ask Q43

42. Do you have any of WeChat/Line/Viber/Whatsapp installed on a smartphone you use (i.e. apps for direct messaging friends or family)?
    - Yes
    - No (skip to Q46)
    - No idea (skip to Q46)
    - Refuse to answer (skip to Q46)
43. Did you install any of these apps yourself?
    - Yes
    - No
    - No idea
    - Refuse to answer
44. Were you aware that these apps access all your contacts on your phone?
    - Yes, I know
    - No, I don't know
    - Refuse to answer
45. How much of a privacy problem do you think this practice of accessing all your contacts is? Please use a number between 0 to 10 where 0 means it is no problem at all and 10 means the law should prohibit this.
    - 0-10
    - No idea/ don't know
    - Refuse to answer

Ireland

Survey: Data Protection SME Business Study 2018

1. Does your organisation collect and use personal data? (e.g. employee data such as Payroll etc., database of customer details, etc.)
   - Yes
   - No/ Don't know
2. Is the data you collect and process confined to personal information about your employees or more broad-based to include information about your customers/ clients?
   - Broad-based including information about customers/ clients
   - Both employees and customers/ clients data
   - Employee details only
   - Don't know
3. Are you aware that major changes to data protection law are imminent?
   - Yes
   - No
4. Do you know that the General Data Protection Regulation will be effective from 25th May 2018?
   - Yes
   - No
5. If asked, could you name three changes that the General Data Protection Regulation will mean for your organisation?
   - Yes, I could name three
   - No, but I could name one or two
   - No, I could not name any
6. Do you know, for example, if your organisation will be required to appoint a Data Protection Officer?
   - Yes
   - No/ Don't know
7. Have you identified the steps/ actions that your organisation will need to take to be compliant with the General Data Protection Regulation?
   - Yes
   - No/ Don't know
8. Do you have a staff member(s) who is responsible for overseeing compliance with data protection and preparing for the GDPR?
   - Yes
   - No/ don't know
9. Have you carried out an assessment of all the personal data you hold?
   - Yes
   - No/ don't know
10. Have you carried out an assessment of why you hold personal data?
    - Yes
    - No/ don't know

11. Have you carried out an assessment of how long you need to keep your personal data you hold?
    - Yes
    - No/ Don't know
12. Is data protection included as a consideration in the planning phase of your ongoing and future business activity?
    - Yes
    - No/ Don't know
13. Have you carried out an evaluation to establish whether or not the nature of your company's processing requires you to carry out a Data Protection Impact Assessment?
    - Yes
    - No/ Don't know
14. Have you developed a data protection risk register to help identify and mitigate data protection risks?
    - Yes
    - No/ Don't know
15. Are you using, or planning to use, an outside resource to help your organisation prepare for the General Data Protection Regulation?
    - Yes
    - No/ don't know
16. And, what type of service provider are you using or planning to use? Please all that apply.
    - Yes (don't know, law firm, consultancy firm, other outside source (please specify))
    - No/ don't know
17. Are you aware of some of the penalties that can be imposed on companies for failing to comply with the General Data Protection Regulation?
    - Yes
    - No
18. To what extent do you think data protection compliance is a priority in your organisation at owner/ boardroom/ senior management level?
    - High priority
    - Priority
    - Neither/ nor
    - Low priority
    - Not a priority at all
19. Have you actioned your GDPR implementation plan?
    - Yes
    - No/ Don't know
20. What format of guidance would you find most helpful to your preparations for the General Data Protection Regulation?
    - Web-based guidance
    - Downloadable PDF guidance
    - Hardcopy guidance
    - Video clips/ animations
    - Infographics

- Other (please specify)
- Don’t know

Israel

Survey:

1. Which categories of personal data do you consider highly sensitive and private (for example: financial data)
2. Which categories, of personal data, would you consider as not secure enough and might be subject to breaches?

In the following questions you'll be presented with different sectors in which personal data is being collected and processed. Please indicate the level of sensitivity that you think should be attributed to each category and what is the level of risk and probability that the data may be breached/leaked?

3. Health data (for example: medical data in hospitals, HMO and etc.)
   - Data sensitivity
     Very sensitive – sensitive – low sensitivity – very low sensitivity – not sensitive at all – don't have an opinion on this
   - Risk of data breach/ data leakage
     High – medium – low – no risk – don't have an opinion
4. Financial data (for example: banks, credit card companies, insurance companies etc.)
   - Data sensitivity
     Very sensitive – sensitive – low sensitivity – very low sensitivity – not sensitive at all – don't have an opinion on this
   - Risk of data breach/ data leakage
     High – medium – low – no risk – don't have an opinion
5. Educational data (schools, universities, etc.)
   - Data sensitivity
     Very sensitive – sensitive – low sensitivity – very low sensitivity – not sensitive at all – don't have an opinion on this
   - Risk of data breach/ data leakage
     High – medium – low – no risk – don't have an opinion
6. Welfare data (social security payments etc.)
   - Data sensitivity
     Very sensitive – sensitive – low sensitivity – very low sensitivity – not sensitive at all – don't have an opinion on this
   - Risk of data breach/ data leakage
     High – medium – low – no risk – don't have an opinion
7. Internet and mobile phones data (for example the browsing data, location data, etc.)
   - Data sensitivity
     Very sensitive – sensitive – low sensitivity – very low sensitivity – not sensitive at all – don't have an opinion on this
   - Risk of data breach/ data leakage
     High – medium – low – no risk – don't have an opinion
8. Media providers (the data that TV service providers collect)

- Data sensitivity
  Very sensitive – sensitive – low sensitivity – very low sensitivity – not sensitive at all – don't have an opinion on this
- Risk of data breach/ data leakage
  High – medium – low – no risk – don't have an opinion

9. Apps (the data collected by the application you use on your phone)
   - Data sensitivity
     Very sensitive – sensitive – low sensitivity – very low sensitivity – not sensitive at all – don't have an opinion on this
   - Risk of data breach/ data leakage
     High – medium – low – no risk – don't have an opinion
10. Search engines and "Internet Giants" (google, Facebook, amazon etc.)
    - Data sensitivity
      Very sensitive – sensitive – low sensitivity – very low sensitivity – not sensitive at all – don't have an opinion on this
    - Risk of data breach/ data leakage
      High – medium – low – no risk – don't have an opinion
11. Retail data (data that retail chains collect through member cards, consumer habits, etc.)
    - Data sensitivity
      Very sensitive – sensitive – low sensitivity – very low sensitivity – not sensitive at all – don't have an opinion on this
    - Risk of data breach/ data leakage
      High – medium – low – no risk – don't have an opinion
12. Municipal data (the information local municipalities collect about you)
    - Data sensitivity
      Very sensitive – sensitive – low sensitivity – very low sensitivity – not sensitive at all – don't have an opinion on this
    - Risk of data breach/ data leakage
      High – medium – low – no risk – don't have an opinion

Korea

Personal Information Protection Commission

Survey: Survey on Public Awareness of Data Protection

1. Are you aware of the Personal Information Protection Act?
    - Aware of it
    - Well of aware of it
    - Have heard of it
    - Don’t know
2. Are you aware of the Personal Information Protection Commission?
    - Aware of it
    - Well of aware of it
    - Have heard of it
    - Don’t know

Korea

Korea Internet & Security Agency

Survey: 2016 Survey on information security – individual

1. Awareness of the importance of information security
2. Awareness of the Importance of Personal Information Protection
3. Awareness of Information Security Threats
   - Leakage of personal information and violation of privacy (personal information, photos, videos, etc.)
   - Damage from malware infection(virus, adware, spyware) (information loss, physical and time damage)
   - Financial damage from phishing, pharming, smishing (fraudulent message, fake websites)
   - Financial damages from credit or debit card fraud, or illegal payments
   - Damages from ransomware infection (information loss, physical and time damage)
4. Types of Interested Information on Information Security
   - Detailed experiential information and ways to prevent and respond to damages
   - Information related to information security products and services
   - Information on the latest information protection and damage issues (damage size, breach types, possibility, etc.)
   - Consultation and reporting information when damages happen
   - Information and reports and websites detailing user damages and responses
   - Learning and certification on information protection
5. Information Collection and Education on Information Security
   - Information search on information protection (TV, newspaper, internet, etc.)
   - Acquisition of information from acquaintances, friends, and colleagues
   - Inquiries about information protection to private companies (vaccine companies, information security companies, etc.)
   - Inquiries about information protection to public institutions (MSIP, KISA, Police Cyber Terrorism Centre, etc.)
   - Purchase print materials on information protection (books, educational SW, contents, etc.)
   - Take classes on information protection (internet lectures, seminars, academic conferences, etc.)
6. Major Obstacles of Information Collection Related to Information Security
   - Terms related to information protection are unfamiliar and difficult
   - There is too much complex information
   - Information is updated too quickly to follow
   - Lack of information protection material that is required
   - Lack of knowledge on where to acquire the information
7. Use of Information Security Products
8. Use of Information Security Software - Users of Information Security Products
   - Security software mounted on the OS (Windows Defender, etc.)
   - Security software provided by internet service providers (ISP) (KT olleh Doctor, SK Broad&Clean, LG U+ Internet V3, etc.)

- Other paid software (V3 365 Clinic, Norton, etc.)
- Other free software (Public Alyac, V3 Lite, etc.)

9. Frequency of Malicious Code Scanning (%) – Among Users of an Anti-Virus Program
   - Daily
   - Twice a week
   - Once a week
   - Twice a month
   - Once a month
   - Once every 3 months
   - Once every 6 months
   - Once a year or less
   - Don't know
10. How to Update an Anti-Virus Program (%) - Information Security Software User
    - Automatic updates
    - Manual updates
    - No updates
11. Operating System Security Updates Method
    - Automatic updates
    - Manual updates
    - No updates
12. Important Data Backup: Do you back import data on your PCs to an external device or server?
13. Preventive Measures for PC and Network Security
    - Not opening attachments to suspicious emails
    - Not accessing unknown websites
    - Not downloading files from unknown websites
    - Using encrypted USB thumb drives and others
    - Security updates for applications (Adobe Flash, Hancom Office, etc.)
    - Check for unnecessary additional programs when installing applications
    - Opt out of share settings for files and folders
    - Designate an account for each user if multiple users use one PC
14. Password Setting – Users Who set Passwords
    - When logging into OS (Windows, etc.)
    - When storing important data files
    - When exiting screensaver
    - When setting shared files and folders
15. Security Incident Experiences
    - Damage from malicious code (virus, worm, adware, spyware, etc.) (data theft, physical/time damage)
    - Personal information theft and privacy violation (personal information, photos, videos, etc.)
    - Financial damages due to phising/ pharming/ smishing (fraudulent messages, fake websites, etc.)

- Damage from ransomware infection (time, physical, and financial damage due to information theft)

16. Incident Response - Users Who Experienced a Security Incident
    - Stronger inspection and prevention by the user
    - Installation of security software
    - Changing previous passwords
    - Stop sharing personal information on the internet
    - Read terms of use when signing up for internet services of software
    - Change internet service provider (KT, SK, Broadband, LGU+, etc.)
    - Other
17. Preventive Measures against Personal Information Breach
    - Manage ID, password, social security number, and protect them from others
    - Take care to not expose financial information such as credit card numbers (not executing financial transaction in internet cafes)
    - Not downloading files haphazardly on the internet
    - Take care not to include personal information uploaded to the internet (P2P, shared folders, etc.)
    - Use personal identity theft check service (notice from the service when personal identity theft occurs)
    - Save public key certificates only on personal portable devices (USB thump drive, external hard drive, smartphone, etc.)
    - Use of e-privacy clean service and check personal information use regularly
18. Types of Response to Personal Information Breach – Users Who Experienced Personal Information Breach
    - Cancel the previous service and use other service with same contents
    - Direct compensation to companies that personal information breach
    - Use e-privacy clean center
    - Report/ consult/ inquire – public institutions related to information security
    - Sue the company for civil and criminal damages
    - Other
19. Cloud Service Users
20. Preventive Measures Against Cloud Service Breach - Cloud Service Users
    - Use the service after checking sharing functions and accessibility
    - Check service terms of use
    - Encrypt important files before sharing them
    - Regularly backup to external devices (USB, external hard drive, etc.) prepare for service failures
    - Completely delete important data and check again when to terminating service use
    - Other
21. Threats to Commercialization of Internet of Things (IoT)
    - Increased threat of personal information theft due to the generation and processing of massive amounts of data
    - Weaknesses to management caused by the connection of various devices
    - Increased strength and possibility of cyberattacks from massive malware infection on devices

- Physical/ financial damages from device failure or error
- Threat of extensive damages from increased connectivity

22. Threats to Expansion of a Big Data Service
    - Overly extensive collection of personal information
    - Unlimited use of collected personal information (promotions, advertisement, etc.)
    - Discrimination from analysis of personal information (customer profiling, categorisation, and discrimination)
    - Big data hacking and resulting personal information theft (voice phising, smishing, etc.)
    - Providing collected/analysed personal information to third parties without user approval
23. Awareness on Security of a Convenience Pay Service
    - Convenience is more important
    - Neutral
    - Security is more important
24. Security Level of Convenience Pay Against Regular Payment Methods – Convenience Pay Users

Macau

The Office for Personal Data Protection

Survey: Research on the level of awareness and needs of privacy amongst secondary and university students 2014

General attitude towards the collection and use of personal data

1. Which of the following entail greater privacy risks
   - Identify thefts
   - Surveillance system
   - Online service/ social networking websites
   - Data breach
   - Smartphone/ application software
   - Identity document photocopies/ scanned copies
   - Overseas data transfers
2. What types of data are you unwilling to reveal to enterprises, organisations or public departments
   - Information regarding family members
   - Financial status
   - Address
   - Genetics data
3. What are the reasons that you are unwilling to provide data
   - Information has no relation with the company or institution
   - It is unnecessary
   - Unwilling to reveal to others their addresses and contact information
   - To prevent crime/ security
4. Which of the following data controllers do you find reliable
   - Charities
   - Credit institutions
   - E-commerce sector
   - Estate agents
   - Financial institutions
   - Government departments
   - Health service providers
   - Insurance companies
   - IT companies
   - Research institutes
   - Retail businesses
   - Social media
5. Which methods do you commonly use for protecting personal data
   - Asking the public or private institution why personal data was required
   - Checking website security before providing personal data
   - Clear search and browse histories
   - Destroying information containing personal data

- Providing false personal data
- Privacy settings configured for social networking websites
- Reading privacy policies and notices
- Refused to provide personal data
- Refused using the applications on mobile devices

[other questions couldn’t be extracted from the results]

Macedonia

Survey: Public survey on awareness in personal data protection

1. Do you know what personal data is?
   - Yes
   - No
   - Don’t know
2. If yes, please state some personal data
   - Personal registration number
   - Health data
   - Working place
   - Parents name
   - Date of birth
   - Living address
   - Name and address
3. How familiar are you with the right of privacy and personal data protection?
   - I am not familiar with it
   - Insufficiently
   - Sufficiently
4. For which personal data (except name and surname) are you mostly worried that be abused?
   - Data pertaining to sex life
   - Biometrical data
   - Genetic data
   - Political, religious and other beliefs data
   - Nationality
   - Health data
   - Personal registration number
   - Other
5. Has your personal data been abused?
   - Yes
   - No
   - I don’t know
6. If yes, please state where was your personal data abused
   - Social networks
   - Health institution
   - State body (police)
   - Post
   - Bank
   - Telecommunication operator
   - Other
7. Do you know how you can protect your personal data?
   - No
   - Yes, with criminal charges submitted to the police

- Yes, with initiation of civil proceeding
- Yes, with a submitted request to the Directorate for Personal Data Protection

8. If your personal data have been abused on some of the social networks, do you know how to proceed?
   - Yes, with a submitted request to the Directorate for Personal Data Protection
   - Yes, with initiation of civil proceeding
   - Yes, with criminal charges submitted to the police
   - Yes, by writing to the administrator
   - I don't know
   - Other
9. Have you heard about the directorate for personal data protection and do you know what their competence is?
   - No, I haven't heard and I don't know their competence
   - Yes, I've heard but I don't know their competence
   - Yes, I've heard and I know their competence
10. On which medias have you heard about the directorate for personal data protection?
    - Internet
    - Newspaper
    - TV
    - Other
11. Have you watched any program or read an article about the directorate for personal data protection?
    - No
    - Internet
    - Newspaper
    - TV
12. The following organisations collect your personal data. Do you think they provide appropriate protection?
    - Private companies
    - Local self-government
    - Government institutions
    - Internal revenue service
    - Police
    - Direct marketing companies
    - Insurance companies
    - Banks and financial institutions
    - Telecommunications operators
    - Health institutions

    I don't know – no – yes
13. Do you know your rights when you are under video surveillance?
    - No, I don't know
    - Yes, there should be notification where and how long are kept the recorded videos
    - Yes, there should be name of the controller who is making the surveillance
    - Yes, there should be a notification that you are under surveillance

New Zealand

Survey: Privacy concerns and sharing data 2018

Data Privacy Concerns

1. Using a scale of 1 to 5 where 1 means you are very concerned and 5 not concerned at all, how concerned are you about individual's privacy and the protection of personal information?
2. Looking back over the last few years, have you got more concerned about issues of individual privacy and personal information, less concerned or has your level of concern stayed about the same?
   - More concerned
   - Level of concern stayed the same
   - Less concerned
   - Depends
   - Unsure
3. Using a scale of 1 to 5 where 1 means you are very concerned and 5 not concerned at all, how concerned are you about the following privacy issues in New Zealand today?
   - The information children put on the internet about themselves
   - Businesses sharing your personal information with other businesses without your permission
   - Security of your personal information on the internet
   - Use of drones in residential areas
   - Government agencies sharing your personal information with other government agencies without your permission
   - Health organisation sharing your health information with other health organisations without telling you
   - Use of CCTV by individuals
4. How concerned are you about the following privacy issues in New Zealand today?
   - The information children put on the internet about themselves
   - Businesses sharing your personal information with other businesses without your permission
   - Security of your personal information on the internet
   - Government agencies sharing your personal information with other government agencies without your permission
   - Health organisation sharing your health information with other health organisations without telling you

Privacy commission – awareness ratings

5. Have you heard of the Privacy Commissioner?
   - Yes
   - No
6. Are you aware of the Privacy Act?
   - Yes

- No

Personal data

7. How much, if at all, do you trust government organisations/ companies with your personal data?
   - A great deal
   - A fair amount
   - Not very much
   - Not at all
8. How comfortable if at all, are you with each of the following?
   - Sharing my personal data with a government department online in order to access a service
   - Sharing personal data online with a company in order to perform a transaction (buy something online, book a trip etc.)
   - Sharing personal data about myself online through the use of social media platforms (e.g. Twitter, Facebook..)

     Very comfortable – Fairly comfortable – Not very comfortable – Not at all comfortable – Not applicable – Don't know
9. How confident, if at all, are you that your personal data is used, stored and secured appropriately in each of the following circumstances?
   - When I share personal data with a government department through the use of a government website
   - When I share personal data online to buy goods
   - When I share personal data online through the use of social media platform

     Very confident – Fairly confident – Not very confident – Not at all confident – Not applicable – Don't know
10. You said earlier that you are uncomfortable with online agencies collecting and analysing your personal data. Why do you use free services that analyse your personal data if you feel uncomfortable about it? Which statement is most applicable?
    - Because it is difficult to find alternatives that don't exploit my personal data
    - Because I haven't given it much thought
    - Because I haven't been fully aware of how my data has been used
    - Because I don't see any negative consequences for myself
    - Because I can't bring myself to be concerned about it
    - Other reasons
    - Because everyone else does it
    - I don't know

Norway

Survey 1: Personal data in exchange for free services: an unhappy partnership?

1. Have you noticed advertisements appearing on your screen that are directly related to your activity online (e.g. Searches you have made/ websites you have visited)
   - Yes
   - No
   - Don't know
2. How aware are you of what data concerning you is being collected by different online agencies?
   - Very aware
   - Somewhat aware
   - Somewhat unaware
   - Very unaware
   - Don't know
3. How aware are you of how these agencies use information about you in order to present you with targeted advertisements
   - Very aware
   - Somewhat aware
   - Somewhat unaware
   - Very unaware
   - Don't know
4. Websites use information capsules called cookies to track users' online activity to tailor advertising to each individual user. An information capsule/ cookie is a small text file used to obtain information on who you are based on the pages you visit and what you read online. How many cookies do you think are placed into your web browser when you visit the front page of Aftenposten.no?
5. I find it uncomfortable that online agencies collect and analyse my personal data, and share it with other companies to provide me with targeted advertisements
   - Strongly agree
   - Somewhat agree
   - Somewhat disagree
   - Strongly disagree
   - No opinion/ don't know
6. It is OK that members receive a lower price than other customers because the shop can monitor their purchasing habits
   - Strongly agree
   - Somewhat agree
   - Somewhat disagree
   - Strongly disagree
   - No opinion/ don't know
7. It is OK for a free email service provider to read the content of my emails to provide targeted advertisements
   - Strongly agree

- Somewhat agree
- Somewhat disagree
- Strongly disagree
- No opinion/ don’t know

8. It is OK that online newspapers keep track of everything I read in a newspaper to provide targeted advertisements
   - Strongly agree
   - Somewhat agree
   - Somewhat disagree
   - Strongly disagree
   - No opinion/ don’t know
9. Free online services such as newspapers and social media are funded by showing users advertising. Some of them analyse users’ personal data to provide advertisements that are individually tailored to that user. Do people really want personalised advertising rather than more random advertising, which can be perceived as less relevant?
   - Random advertising
   - Targeted advertising
10. Suppose that revenue for providers of free services such as email and social networking sites was not generated through targeted advertising. Would we willing to pay for these services out of our own pockets instead?
    - Yes
    - No
    - Don’t know
11. How much will people be willing to pay?
12. What is the most important reason for which you are willing to pay?
    - to avoid advertisements
    - to ensure that as little as possible of my personal data is collected and analysed
    - other
    - don’t know

Survey 2 – It's getting personal

1. I welcome a development where my insurance premium is calculated on the basis of sensor generated information about my day-to-day life and behaviour
   - Agree
   - Indifferent
   - Disagree
   - Don't know
2. Given a significantly lower premium, I would have no problem giving the insurance company access to detailed sensor-generated data about my day-to-day life and behaviour
   - Agree
   - Indifferent
   - Disagree
   - Don't know
3. I want my insurance company to take an active role with regard to my health, for example by sending me text messages when I do too little exercise or offering personalised tips on healthy living
   - Agree
   - Indifferent
   - Disagree
   - Don't know
4. What would you think if credit rating companies gave a good or bad credit rating depending on your online activity, for example which websites you have visited, what you have posted on social media and what you have bought online?
   - Positive
   - Indifferent
   - Negative
5. Would you be interested in using a helpful banking service from Google or Facebook?
   - Yes
   - No
   - Don't know/ other

Survey 3: Privacy survey - Collective Report from the Privacy Survey 2013/2014

1. To what extent are you busy you are in privacy?
   Alternatives:
   - Highly concerned with privacy
   - Pretty concerned with privacy
   - Slightly concerned with privacy
2. Have you become more or less concerned with privacy over the last two to three years?
   Alternatives:
   - More busy than before
   - As busy as before
   - Less busy than before
   - Do not know
3. Are there any information about you or others that you think the law should specifically protect against collection and further use? How important is that the law protects:
   - Information about your health
   - Your genes / DNA (information on inheritance and likelihood of various diseases)
   - Your social security number / social security number - 11 digits
   - Your political opinion
   - Your religious opinion
   - Information about your private economy
   - Which trade union you are a member of
   - Information about places you have been and where you are moving
   - Which websites you have visited / viewed
   - Pictures of you
   - Who you communicate with on phone and email
   - The content of the phone calls and your e-mail
   - What you have searched for on search engines
   - Measurements of your efficiency and time spent at work
     Alternatives:
   - Completely unimportant
   - A little important
   - A little important
   - Very important
   - Do not know
4. Google Glass (Google Glasses) comes to Norway in a short period of time. The glasses are used by speaking its wishes and commands. Information is displayed in a corner of the spectacles. The information is based on-site and personal preferences and habits. The glasses can be used, for example to take pictures, film and talk to others. Check if you see for yourself that you might find it useful to Use Google glasses for these purposes:
   More options possible [Randomiser]
   - Record video of a dangerous traffic situation (e.g. a bypass)
   - Record video from a lecture or lecture
   - Stream / stream video from a concert

- Record video while walking on the street
- Receive tips that a store in the immediate area leads the product you are looking for
- Ask the glasses to help you recognize people you do not recognize yourself
- None of these [Exclusive]
- Do not know [Exclusive]

5. Below is a list of services / technologies that we ask you to answer if you are a private user today, you would like to use or could not imagine using.
   - GPS tracking of your children
   - GPS tracking of elderly or other family members with special care needs
   - Camera surveillance inside or outside your own home or cabin
   - Camera in a car that films out of the car
   - Helmet or action camera (eg bike, slalom or other places)
   - Recording your phone calls
   - Drones or radio controlled helicopters like movies or taking pictures from the air
   - Google glasses

   Alternatives:
   - Uses today
   - Could imagine using
   - Could not imagine using
   - Do not know
6. Body-tight technology is technology built into bracelets, watches, jewellery, clothes or patches. You barely notice that you have them on you and they can do regular measurements of e.g. number of steps, location, heart rate, body temperature, sleep rhythm, calorie consumption. Would you be willing to share your own data from the use of this kind of technology with the following?
   - The police - if I need help
   - The ambulance - in an acute situation
   - Fast doctor - for help with sleep problems
   - The doctor - to keep an eye on my health
   - Employer - to keep an eye on my health
   - Friends - to motivate me to train more

   Alternatives:
   - Yes
   - Maybe
   - No
   - Do not know
7. Below is a list of private and public organizations and businesses that may have personal information about you. How big or small trust you have in the way they store and use personal information on?
   - Healthcare
   - Insurance companies
   - Credit information companies
   - Banker
   - Telecommunications companies
   - Employers (generally speaking)

- Social websites
- Police
- The Norwegian intelligence services
- NAV
- Taxation
- Municipalities
- Online stores

  Alternatives:
- No trust
- Little trust
- Some trust
- Great trust
- Do not know

8. Below is a list of events. Check for the two you are most worried about. [Randomization]
   - Unwanted image publishing - That someone, without asking you, publishes images or text on the web as gives an unfavorable or false impression of you
   - Hacking / Theft - Someone steals or hacks your mobile or computer and accesses that which is stored there
   - Snoking - That employees illegitimate look in private information a public or private business has about you, such as health records or bank statements
   - Police / intelligence surveillance - That authorities like police or intelligence collect and Checks information about you, even if you have not done anything wrong
   - Surveillance from government agencies- That authorities like NAV, the tax administration and the customs authorities collect and checks information about you, even if you have not done anything wrong
   - Identity Theft - Someone pretend to be you, to gain an economic gain, or to do hurt
   - Lack of control - I do not have an overview of which companies have the personal information mine and what they are used to
   - Sensitive personal information on the way - Unauthorized person through data interruption, leakage or errors with a private or public sector can access information about you
9. Camera surveillance can be analysed to recognize faces or to estimate a person age and gender. How positive or negative are you for the use described below?
   - Video recording of you in a store is analysed to show a display in the store advertising that suits your appearance, gender, and age.
   - Monitoring facilities at railway stations and airports analyse everyone in order to discover wanted people.
   - At workplace surveillance facilities recognize and register employees so that employer can know where each one is at all times.

   Alternatives:
   - Very negative
   - A little negative
   - Neither or
   - A little positive

- Very positive
- Do not know

10. How positive or negative are you for camera surveillance at the following locations:
    - Inside the bus or train
    - In taxis
    - In banking and post offices
    - In bars and restaurants
    - By the sinks in public toilets
    - In stores
    - At the entrance to your own workplace or school / study place
    - Where you do your assignments / studies
    - In parks, on beaches and other public recreation areas
    - On the street
    - In the waiting room at the emergency room

    Alternatives:
    - Very negative
    - A little negative
    - Neither or
    - A little positive
    - Very positive
    - Do not know
11. How important or unimportant it is for you that you can be anonymous (that you do not leave online track that tells you what you've done or where you've been) when you ...
    - Travel collectively by bus, subway, train, tram
    - Driving a car
    - Pay for goods and services
    - Surf the internet
    - Goes streetlong

    Alternatives:
    - Not important at all
    - A little important
    - Important
    - Very important
    - Do not know
    - Not applicable
12. Have you perceived that personal information about you has been lost or misused others?

    Alternatives:
    - Yes
    - No
    - Do not know
13. Have you experienced that someone else has posted a picture or other information about you online like you not wanted to be shared?

    Alternatives:
    - Yes

- No
- Do not know

14. Have you ever asked to know what information about you exists registered in a private or public company?
    Alternatives:
    - Yes
    - No
    - Do not know
15. Think of situations where you provide personal information to a company that will register them its systems. Examples may be when entering into a service agreement, upon registration of one user account on a web service or at a purchase in an online store. To what extent do you perceive that businesses inform you about how your personal information will get used?
    Alternatives:
    - Always
    - Often
    - Occasionally
    - Rarely
    - Never
    - Do not know
16. A privacy statement is a description of how the business processes personal data. If you consider using a service, the business website would have one Privacy Policy ...
    Alternatives:
    - Count positively
    - Count negatively
    - Do not matter
    - Do not know
17. Do you use one or more social networking communities?
    Alternatives:
    - Yes, weekly
    - Yes, but less often
    - No
    - Do not know
18. (Filter: Question 17 = 1 OR 2 (Yes, using social networking weekly or less frequently)) Social online communities analyse your online habits and preferences to map you, including so that Advertisers can offer you customized advertising. Would you like to pay $ 100 a month to avoid the social networking you use map and analyse your personal information?
    Alternatives:
    - Yes, I would have been willing to pay $ 100 a month
    - No, I would not pay 100 kr per month
    - Do not know
19. Someone sometimes lets others use their personal accounts online, for example, to make one pay or send the tax return separately. Have you volunteer given login

information like password, pin-codes, code calculator for any of these the services of someone else?
Check all relevant options. [Randomization]
- Email account
- Netbank
- Public portal (eg tax return, childcare application and more)
- Online store
- Social networking
- None of these [Exclusive]
- Do not know [Exclusive]

20. Do you want to be notified if your personal information comes from a private or public sector in awe, for example through a data interruption?
Alternatives:
- Yes
- No
- Do not know

21. Have you done any of the following activities just because you are unsure of how the information you leave again can be used later?
Check for all relevant options. [Randomization]
- Failed to make a search (by a person, term, thing) online
- Failed to make a purchase
- Failed to sign a call / support campaign because it can be posted online
- Rather than having an oral conversation than communicating electronically (eg SMS, email,chat)
- Payed cash instead of using cards where the goods purchases are registered
- Failed to inform about critical circumstances because it may be linked to you as informer
- Signed out of a social networking community
- Other, notes_____
- No, have not done any of these activities [Exclusive]
- Do not know [Exclusive]

22. Have you heard of the surveillance case where Edward Snowden revealed that American Security authorities have access to large amounts of personal information about European citizens via telecommunications and internet companies?
Alternatives:
- Yes
- No
- Do not know

23. After hearing about the US Monitoring, which of the following statements suits best for you?
Alternatives:
- I think this surveillance is unproblematic
- I think this surveillance is unacceptable
- I think this surveillance is worrying, but necessary
- I have no particular opinion on this matter

- Do not know

24. (Filter: Yes in Qty 22)
    After hearing about the US surveillance, some of the following claims apply You?
    More choices possible. [Randomization]
    - I have thought about an extra time before using certain words in e-mail, in one phone call or in an Internet search
    - I have thought about the possibility that foreign intelligence services catch up on mine online activities
    - I have changed the use of certain services and / or communication channels
    - I have stopped using certain services and / or communication channels
    - This case has not affected my actions
    - I have adapted to me in other ways, notes: _____
    - None of these [Exclusive]
    - Do not know [Exclusive]
25. Look for a hypothetical situation: Norwegian and foreign intelligence monitors and stores all Norwegian citizens' electronic communications and networking (eg email, social networking, website search, search). Which of these statements suits you:
    Check all relevant options. [Randomization]
    - I would have been more careful about how I formulated
    - I would have been more careful about who I communicate with
    - I would have been more careful about what I'm searching for online
    - I would have been more careful to sign up for calls / campaigns
    - I would have been more careful about what I'm saying on social networking and debating online
    - It does not matter to me, I continue as before
    - None of these [Exclusive]
    - Do not know [Exclusive]
26. Imagine the following situation: Norwegian and foreign intelligence monitors and stores who you send to and receive emails from time and subject fields, but not the content itself. How intervention seems you this is?
    Alternatives:
    - 1 - not intervention at all
    - 2
    - 3
    - 4
    - 5 - highly interventive
    - Do not know
27. Which of these has the greatest influence over your privacy being taken care of?
    Ranger from 1 (greatest influence) to 3 (least influence):
    - The authorities that administer the regulations
    - Myself through my choices
    - The companies that have information about me
28. How do you agree or disagree with the allegations?
    [Randomization]

- Public agencies, such as health care, nav and police should be free to exchange personal data between themselves to reveal those who utilize welfare systems.
- It is impossible to have an overview of anyone who has information about me and how the information is used.
- Only those who have something to hide need privacy.
- Public agencies should be free to exchange information about individuals in order to offer the most effective services possible.
- If I publish something on social websites or open online, I have to find that others use the information for something completely different without asking me.
- The hospital, my general practitioner and others who treat me should be free to exchange my health information without asking me first.
- We should allow stronger privacy interventions to fight crime.
- The police and security authorities should be able to monitor and use open information from social media, blogs and other internet services, for prevention and investigation, even if the surveillance includes you.
- The state should store a DNA profile of all newborns for use later police investigations
- Health researchers should be able to use information from people's patient records without it individual consent.
- Good privacy is a prerequisite for a free and democratic society.

Alternatives:

- Totally disagree
- Partially disagree
- Neither or
- Partially agree
- Fully agree
- Do not know

Survey 4 – Chilling down in Norway

1. Are there certain things you have decided not to do because you are not sure how the information may be used in the future?
   - No, I have not done any of these
   - Left social online community
   - Not reported unacceptable conditions because this action may be linked to you as the informant
   - Paid cash rather than use a bank card because the purchases will be registered
   - Decided to talk face-to-face rather than communicate electronically (e.g. text message, e-mail, chat)
   - Not signed a petition because it may be made available on the internet
   - Decided not to make a purchase
   - Decided not to do a web search
2. After you learned about the US surveillance, do you agree with any of the statements below?
   - This case has not had any impact on my conduct
   - I have considered the possibility that foreign intelligence services may register my …
   - I have thought more carefully about using certain words in e-mails, in telephone …
   - I have changed the way I use certain services and communication channels
   - I have made adjustments in other ways
   - None of the above
   - Do not know
3. Envision a hypothetical situation: Norwegian and foreign intelligence services register and store all electronic communications and use of the Internet by Norwegian citizens (e.g. e-mails, activities in social networks, searches). If so which of these statements
   - Would be of no consequence for me, I would continue as before
   - I would have been more careful about what kind of searches I would do on the Internet
   - I would have been more careful about what I said in social online communities and in debates on …
   - I would have been more careful about signing petitions/campaigns
   - I would have been more careful about how I said things
   - I would have been more careful about which people I would communicate with
   - None of the above
   - Do not know

Peru

Survey: Anonymous survey about data protection

1. Have you ever received, any calling, e-mail and/or letter in your address, from any company of which you are not a costumer or which you never gave your data (telephone number, e-mail or address)?
   - Yes
   - No

   If your answer is "Yes", tell us to which of these categories belongs that company from who received that calling, e-mail or letter (you can mark more than a single option, if is necessary):
   - Bank and credit companies
   - General stores
   - Hospitals and health services
   - Insurance companies
   - Travel agencies
   - Markets
   - Restaurants
   - Educational institutions
   - Telecommunication companies
   - Polling and survey companies
   - Others
2. Have you ever received, from any company of which you are a costumer, any calling, e-mail and/or letter in your address, with offers or advertising of good and services unrelated to that you have purchased?
   - Yes
   - No

     If your answer is "Yes", tell us to which of these categories belongs that company from who received that calling, e-mail or letter (you can mark more than a single option, if is necessary):
   - Bank and credit companies
   - General stores
   - Hospitals and health services
   - Insurance companies
   - Travel agencies
   - Markets
   - Restaurants
   - Educational institutions
   - Telecommunication companies
   - Polling and survey companies
   - Others
3. Do you think that your data (telephone number, e-mail, home address, health data, etc.) has been managed or used improperly or in an illegal way?
   - Yes

- No

If your answer is "Yes", tell us to which of these categories belongs that company which managed or used your data improperly or in an illegal way (you can mark more than a single option, if is necessary):

- Bank and credit companies
- General stores
- Hospitals and health services
- Insurance companies
- Travel agencies
- Markets
- Restaurants
- Educational institutions
- Telecommunication companies
- Polling and survey companies
- Others

If you remember, tell which company(ies) managed or used your data improperly or in an illegal way:

- Bank and credit companies
- General stores
- Hospitals and health services
- Insurance companies
- Travel agencies
- Markets
- Restaurants
- Educational institutions
- Telecommunication companies
- Polling and survey companies
- Others

Describe briefly what the improper or illegal management or use of your data consist of:

4. Which categories of companies do you think develop activities that could damage privacy of any people?
   - Bank and credit companies
   - General stores
   - Hospitals and health services
   - Insurance companies
   - Travel agencies
   - Markets
   - Restaurants
   - Educational institutions
   - Telecommunication companies
   - Polling and survey companies
   - Others

Philippines

Filipino public opinion on data privacy and attitudes and behaviour towards internet usage

1. If you hear the term “PERSONAL DATA PRIVACY”, what is the first thing that comes to your mind? (open- end one answer only)
2. The Data Privacy Act of 2012 is a law that aims to protect the personal information of citizens that was gathered by the government and the private sector. Have you heard or read anything regarding this law, or you only heard or read about this now?
   - Have you heard or read about this (continue)
   - Heard or read about this just now (go to Q6)
3. Those who are aware of the Data Privacy Act of 2012 what is your source of information about the Data Privacy Act 2012
   - Television
   - Facebook, Twitter, YouTube
   - Radio
   - Newspaper
   - Friends/acquaintances
   - Government personnel
   - Family
   - Brochures, leaflets, pamphlets and other similar print material
   - Own experience
   - Others, please specify
4. The National Privacy Commission or NPC is the primary government agency tasked by The Data Privacy Act of 2012 to safeguard and protect the personal information of citizens that was gathered by the government and the private sector. Have you heard or read anything regarding this agency, or you only heard or read about this now?
   - Have you heard or read about this (continue)
   - Heard or read about this just now (go to Q8)
5. If you have heard or heard about the NPC: You can tell how satisfied or dissatisfied with the performance of the National Privacy Commission. Are you
   - Satisfied
   - Dissatisfied
   - Undecided
6. Those who are aware of NPC what is your source of information about the NPC
   - Television
   - Radio
   - Newspaper
   - Facebook, Twitter, Youtube
   - Friends/ acquaintances
   - Family
   - Own experience
   - Brochures and leaflets
   - Internet

- Google
- Law firm/ office

7. Have you heard or read, at any time, regarding this decision by the National Privacy Commission or NPC regarding the hacking on the Comelec's website or is it just now heard?
   - Aware
   - Not aware
8. Do you agree or disagree with the decision of the National Privacy Commission or NPC regarding the alleged hacking of the Comelec website?
   - Agree
   - Disagree
   - Undecided
9. Have you heard or read, at any time, about the right to damages by the data subject, or you just heard it
   - Aware
   - Not aware
10. Have you heard or read, at any time, about the right to reasonable access by the data subject, or you just heard it
    - Aware
    - Not aware
11. Have you heard or read, at any time, about the right to object by the data subject, or you just heard it
    - Aware
    - Not aware
12. Have you heard or read, at any time, about the data subject's right to be informed, or you just heard it
    - Aware
    - Not aware
13. Have you heard or read, at any time, about the data subject's right to erasure or blocking, or you just heard it
    - Aware
    - Not aware
14. If you have all the rights to the data subjects we have discussed earlier, how important are your rights in your life? Are these ...
    - Important
    - Not important
    - Undecided
15. If you feel that your personal information is used incorrectly, disclosed with maliciousness, or erased in the wrong manner, or any of your data subject rights violated, in which office, agency or institution you will file complaint? Where are you?
    - LGUs
    - Police
    - NBI
    - Lawyers
    - Trial Courts

- DSWD
- COMELEC
- CHR
- President/ Government
- NPC
- Media
- DOJ
- DILG
- Ombudsman
- NTC
- DOLE
- NSO
- Others
- None/ don't know/ Can't say

16. Those that are aware of the 9 listed Government organisations holding personal information how much trust do you have in them holding personal information?
    - Philippine health insurance corporation
    - National bureau of investigation
    - Social security system
    - Department of foreign affairs
    - Government service insurance system
    - Bureau of Internal Revenue
    - Commission on Elections
    - Philippine Postal Corporation
    - Land Transportation Office

    Much trust – little trust – undecided
17. Those that are aware of the 6 listed private institutions holding personal information, how much trust do you have in them holding personal information?
    - Schools
    - Hospitals/ clinics
    - Banks
    - GLOBE
    - SMART
    - Credit card companies

    Much trust – little trust – undecided
18. Those that are aware of the 6 listed social media holding personal information, how much trust do you have in them holding personal information?
    - Facebook
    - Yahoo
    - Instagram
    - Gmail
    - Twitter
    - Viber

    Much trust – little trust – undecided
19. Rate the degree of sensitivity of personal information

- Salary/ other benefits
- Phone number
- Home address
- Name
- Place of work
- Birthday
- Email address
- Physical location
- Name of spouse
- Place of birth
- Name of parents
- Sex
- Citizenship

Sensitive – not sensitive – undecided

20. Rate the degree of sensitivity of sensitive personal information
    - Signature
    - Credit card/ bank account numbers
    - Social security number
    - Fingerprint
    - PHILHEALTH number
    - Licenses
    - Tax Identification Number
    - Tax returns
    - Picture
    - Websites visited
    - Age
    - Religion
    - Basic purchasing habits
    - Political affiliation
    - Marital status
    - Relationship history
    - Online searches
    - Race
    - Educational attainment
    - Ethnic origin
    - Height
    - Weight

    Sensitive – not sensitive – undecided
21. Rate the degree of sensitivity of privileged information
    - Court cases
    - State of health

    Sensitive – not sensitive – undecided
22. Do you currently have a social security system ID?
    - Yes

- No

23. Those that are members of SSS, did their personnel tell you where they will use the personal information they got from you?
    - Yes
    - No
24. Whether the information the respondent has given during application for SSS was
    - Too much
    - Too few
    - Just right
25. Information that should not be included when applying for SSS
    - Height
    - Weight
    - Distinguished features
    - TIN
    - Purpose of application
    - E-mail address
    - Phone number
    - Name of parents
    - Picture
    - Marital status
    - Date of birth
    - Sex
    - Signature
    - Fingerprints
    - Name
    - Address
26. Do you currently have a Government Service Insurance System ID?
    - Yes
    - No
27. Did their personnel tell you where they will use the personal information they got from you?
    - Yes
    - No
28. Whether the information the respondent has given during the application for GCIS was
    - Too much
    - Too few
    - Just right
29. Information that should not be included when applying for GSIS
    - Phone number
    - Email address
    - Height
    - Weight
    - Preferred servicing bank
    - Purpose of application
    - Name of parents

30. Do you currently have a driver's license?
    - Yes
    - No
31. Did their personnel tell you where they will use the personal information they got from you?
    - Yes
    - No
32. Whether the information the respondent has given during application for driver's license was
    - Too much
    - Too few
    - Just right
33. Information that should not be included when applying for driver's license
    - Hair colour
    - Complexion
    - Eye colour
    - Built
    - Height
    - Drug test
    - Educational attainment
    - Weight
    - Blood type
    - Office name and address
    - Taxpayer identification number
    - Phone number
    - Name of parents
    - Nationality
    - Place of birth
    - Date of birth
    - Eye test
    - Spouse name
    - No answer
34. Do you currently have a tax identification number?
    - Yes
    - No
35. Did their personnel tell you where they will use the personal information they got from you?
    - Yes
    - No
36. Whether the information the respondent has given during the application for TIN was
    - Too much
    - Too few
    - Just right
37. Information that should not be included when applying for TIN
    - Spouse's employers name

- Nationality
- Date of birth of qualified dependent children
- Spouse's employment status
- Phone number
- Spouse's TIN
- Name of qualified dependent children
- Spouse's employer's TIN
- Spouse name
- Marital status
- Picture
- No answer

38. Do you currently have a PhilHealth ID?
    - Yes
    - No
39. Did their personnel tell you where they will use the personal information they got from you?
    - Yes
    - No
40. Whether the information the respondent has given during the application for PhilHealth was
    - Too much
    - Too few
    - Just right
41. Information that should not be included when applying for PhilHealth
    - Ownership of foreign passport
    - Method of citizenship acquirement
    - Office name and address
    - Present occupation
    - Nationality of parents
    - Nationality of spouse
    - Name of parents
    - E-mail address
    - Phone number
    - Nationality
    - Spouse name
    - Picture
    - Fingerprints
    - Place of birth
    - Name
    - Sex
    - Date of birth
    - Address
    - Signature
    - Marital status
42. Do you currently have a passport?

- Yes
- No

43. Did their personnel tell you where they will use the personal information they got from you?
    - Yes
    - No
44. Whether the information the respondent has given during application for passport was
    - Too much
    - Too few
    - Just right
45. Information that should not be included when applying for passport
    - Age of children below 21 years old
    - TIN
    - Name of children below 21 years old
    - Sex of children below 21 years old
    - Marital status
    - Date of birth of parents
    - Name of parents
    - Date of birth of spouse
    - Nationality
    - Sex of spouse
    - Place of birth
    - Spouse name
46. Would you like to know where the personal information you have provided during your transaction or application will be used?
    - Like to know
    - Does not like to know
47. In your opinion, which of the following personal information should be included in when applying for a telephone or cell phone line
    - Name
    - Home address
    - Phone number
    - Birthday
    - Sex
    - Place of work
    - Place of birth
    - Citizenship
    - Name of spouse
    - Email address
    - Salary and other benefits
    - Physical location
    - Name of parents
48. In your opinion, which of the following sensitive personal information should be included in when applying for a telephone or cell phone line
    - Signature

- Credit card/ bank account numbers
- Social security number
- Fingerprint
- PHILHEALTH number
- Licenses
- Tax Identification Number
- Tax returns
- Picture
- Websites visited
- Age
- Religion
- Basic purchasing habits
- Political affiliation
- Marital status
- Relationship history
- Online searches
- Race
- Educational attainment
- Ethnic origin
- Height
- Weight

49. In your opinion, which of the following privileged information should be included in when applying for a telephone or cell phone line
    - State of health
    - Court cases
50. In your opinion, which of the following personal information should be included in when applying for an internet line
    - Name
    - Home address
    - Phone number
    - Birthday
    - Sex
    - Place of work
    - Place of birth
    - Citizenship
    - Name of spouse
    - Email address
    - Salary and other benefits
    - Physical location
    - Name of parents
51. In your opinion, which of the following sensitive personal information should be included in when applying for an internet line
    - Signature
    - Credit card/ bank account numbers

- Social security number
- Fingerprint
- PHILHEALTH number
- Licenses
- Tax Identification Number
- Tax returns
- Picture
- Websites visited
- Age
- Religion
- Basic purchasing habits
- Political affiliation
- Marital status
- Relationship history
- Online searches
- Race
- Educational attainment
- Ethnic origin
- Height
- Weight

52. In your opinion, which of the following privileged information should be included in when applying for an internet line
    - State of health
    - Court cases
53. In your opinion, which of the following personal information should be included in when applying for a new bank account
    - Name
    - Home address
    - Phone number
    - Birthday
    - Sex
    - Place of work
    - Place of birth
    - Citizenship
    - Name of spouse
    - Email address
    - Salary and other benefits
    - Physical location
    - Name of parents
54. In your opinion, which of the following sensitive personal information should be included in when applying for a new bank account
    - Signature
    - Credit card/ bank account numbers
    - Social security number

- Fingerprint
- PHILHEALTH number
- Licenses
- Tax Identification Number
- Tax returns
- Picture
- Websites visited
- Age
- Religion
- Basic purchasing habits
- Political affiliation
- Marital status
- Relationship history
- Online searches
- Race
- Educational attainment
- Ethnic origin
- Height
- Weight

55. In your opinion, which of the following privileged information should be included in when applying for a new bank account
    - State of health
    - Court cases
56. In your opinion, which of the following personal information should be included in when applying for a credit card
    - Name
    - Home address
    - Phone number
    - Birthday
    - Sex
    - Place of work
    - Place of birth
    - Citizenship
    - Name of spouse
    - Email address
    - Salary and other benefits
    - Physical location
    - Name of parents
57. In your opinion, which of the following sensitive personal information should be included in when applying for a credit card
    - Signature
    - Credit card/ bank account numbers
    - Social security number
    - Fingerprint

- PHILHEALTH number
- Licenses
- Tax Identification Number
- Tax returns
- Picture
- Websites visited
- Age
- Religion
- Basic purchasing habits
- Political affiliation
- Marital status
- Relationship history
- Online searches
- Race
- Educational attainment
- Ethnic origin
- Height
- Weight

58. In your opinion, which of the following privileged information should be included in when applying for a credit card
    - State of health
    - Court cases
59. In your opinion, which of the following personal information should be included in when applying for loyalty or discount cards
    - Name
    - Home address
    - Phone number
    - Birthday
    - Sex
    - Place of work
    - Place of birth
    - Citizenship
    - Name of spouse
    - Email address
    - Salary and other benefits
    - Physical location
    - Name of parents
60. In your opinion, which of the following sensitive personal information should be included in when applying for loyalty or discount cards
    - Signature
    - Credit card/ bank account numbers
    - Social security number
    - Fingerprint
    - PHILHEALTH number

- Licenses
- Tax Identification Number
- Tax returns
- Picture
- Websites visited
- Age
- Religion
- Basic purchasing habits
- Political affiliation
- Marital status
- Relationship history
- Online searches
- Race
- Educational attainment
- Ethnic origin
- Height
- Weight

61. In your opinion, which of the following privileged information should be included in when applying for a loyalty or discount cards
    - State of health
    - Court cases
62. In your opinion, which of the following personal information should be included in when shopping online
    - Name
    - Home address
    - Phone number
    - Birthday
    - Sex
    - Place of work
    - Place of birth
    - Citizenship
    - Name of spouse
    - Email address
    - Salary and other benefits
    - Physical location
    - Name of parents
63. In your opinion, which of the following sensitive personal information should be included in when shopping online
    - Signature
    - Credit card/ bank account numbers
    - Social security number
    - Fingerprint
    - PHILHEALTH number
    - Licenses

- Tax Identification Number
- Tax returns
- Picture
- Websites visited
- Age
- Religion
- Basic purchasing habits
- Political affiliation
- Marital status
- Relationship history
- Online searches
- Race
- Educational attainment
- Ethnic origin
- Height
- Weight

64. In your opinion, which of the following privileged information should be included in when shopping online
    - State of health
    - Court cases
65. In your opinion, which of the following personal information should be included in when applying for a private health insurance
    - Name
    - Home address
    - Phone number
    - Birthday
    - Sex
    - Place of work
    - Place of birth
    - Citizenship
    - Name of spouse
    - Email address
    - Salary and other benefits
    - Physical location
    - Name of parents
66. In your opinion, which of the following sensitive personal information should be included in when applying for a private health insurance
    - Signature
    - Credit card/ bank account numbers
    - Social security number
    - Fingerprint
    - PHILHEALTH number
    - Licenses
    - Tax Identification Number

- Tax returns
- Picture
- Websites visited
- Age
- Religion
- Basic purchasing habits
- Political affiliation
- Marital status
- Relationship history
- Online searches
- Race
- Educational attainment
- Ethnic origin
- Height
- Weight

67. In your opinion, which of the following privileged information should be included in when applying for a private health insurance
    - State of health
    - Court cases
68. Do you currently have ownership/membership of selected private accounts
    - Bank account
    - Loyalty or discount cards
    - Private health insurance
    - Internet line
    - Telephone or cell phone line
    - Credit card
    - Online shopping account
69. If you have: When did you apply (ANSWER IN Q68), did you tell its staff where they use their personal information?
    - Yes
    - No
70. In general, how much do you want to know where to use the required personal information on the transactions or applications you are making?
    - Likes to know
    - Does not like to know
71. Those with a telephone, cell phone or internet line were asked of their trust on telephone, cell phone or internet companies regarding the following five selected transactions
    - It doesn't store the text messages you send
    - It doesn't sell your personal information to other companies
    - It doesn't read the text messages that you send
    - It doesn't record the telephone or cell phone calls you make
    - It doesn't listen to the telephone or cell phone calls you make

    Much trust – little trust – undecided

72. Those with a bank account or a credit card were asked of their trust on banks regarding issues on two selected private transactions
    - It secures your deposited money or credit card from criminals
    - It doesn't sell your personal information to other companies
      Much trust – little trust – undecided
73. Those with a loyalty/ discount cards or online shopping account were asked of their trust on companies offering loyalty/ discount cards or online shopping regarding issues on two selected private transactions
    - They secure your personal information from criminals
    - They do not sell your personal information to other companies
      Much trust – little trust – undecided
74. Those with a private health insurance were asked of their trust on companies selling private health insurance regarding issues on two selected private transactions
    - They secure your personal information from criminals
    - They do not sell your personal information to other companies
      Much trust – little trust – undecided
75. Whether you have personally experienced misuse of your personal data in the past 12 months?
    - Yes, have experienced
    - No , have not experienced
76. What kind of misuse of personal data have you experienced
    - Identity fraud
    - Hacked email/ social media account
    - Damage to reputation
    - Cyber bullying
    - Unauthorised use/ giving of personal information
    - Can't retrieve email/ social media account
    - Incorrect spelling of name
    - Can't remember
77. Who is using your personal information in the wrong way?
    - Friends/ acquaintance
    - Relatives
    - Others
    - Don't know
78. Did you file a complaint to the person or institution who misused your personal data?
    - Yes, filed a complaint
    - No, did not file a complaint
79. Where did you lodge your complaint?
    - Sent a message to the Facebook company
    - Barangay LGU
80. What is the reason why you did not file a complaint?
    - It is too small a thing to bother
    - Let the offense go
    - Both parties had a settlement
    - To avoid further conflict

- Issue was already resolved
- Nothing would be done
- Don’t know where to file a complaint

81. Have you heard or read about the sim card registration 2016 bill, or are you just listening or reading about it now?
    - Yes, aware
    - No, not aware
82. Do you agree or disagree with the SIM Card Registration Act of 2016, the bill that aims to register all pre-paid SIM card cell phones to counter the threats of terrorism and crime?
    - Yes, approve
    - No, disapprove
    - Undecided
83. What information should be included in the proposed SIM Card Registration Act of 2016
    - Name
    - Telephone
    - Home address
    - Age
    - Birthday
    - Signature
    - Sex
    - Picture
    - Fingerprint
    - Religion
    - Citizenship
    - Email address
    - PhilHealth number
    - TIN
    - SSS number
84. Do you go online to get Internet or send or receive emails?
    - Yes
    - No
85. If you use the internet how often do you go online to get Internet or send or receive emails?
    - Daily, +3 hours a day
    - Daily, +2 hours a day
    - Daily, less than an hour a day
    - A few days per week
    - Seldom
86. If you use the internet what equipment or "device" do you use when you are on the internet? Do you use
    - Cell phone
    - Personal computer
    - Laptop
    - Tablet

- Smart TV

87. If you use the internet what is your most commonly used connection when you are online to get Internet or send or receive emails? Are you using
    - Mobile broadband
    - Digital subscriber line or DSL
    - Own Wi-fi
    - Public Wi-fi
88. Do you do the following while you are traveling through a public wi-fi connection?
    - Bills payment
    - Do online banking
    - Make online purchases
    - Send/receive email
    - Uses social media
89. We are concerned about the things you do when you use the Internet. Please tell us if you have done the following Internet activities, or not. Do you
    - Get news
    - Share something online
    - Get information on sensitive health topic
    - Look for a job
    - Play online games
    - Buy things online
    - Study online courses
    - Visit online dating sites
    - Create or work on a blog
90. What personal information is available on the internet?
    - Name
    - Birthday
    - Sex
    - Email address
    - Cell phone/ telephone number
    - Home address
    - Citizenship
    - Place of birth
    - Place of work
    - Name of spouse
    - Details of one's physical location in a particular period
    - Name of parents
    - Salary and other benefits
91. What sensitive personal information is available on the internet?
    - Picture
    - Age
    - Marital status
    - Religion
    - Educational attainment
    - Race

- Things you search online using online search engines
- Height
- Websites that you have visited
- Your basic purchasing habits
- Weight
- Ethnic origin
- Signature
- Political affiliation
- Your relationship history
- Fingerprint
- Social security number
- Licenses
- PhilHealth number
- TIN
- Tax return
- Credit card or bank account numbers

92. What privileged information is available on the internet?
    - The state of your health and the medicines that you take
    - Court cases
93. Have you or your relative, friend or acquaintance experienced online harassment?
    - Yes, being stalked sexually
    - Yes, being harassed sexually
    - Yes, being physically threatened
    - Yes, being purposely embarrassed
    - Yes, being called offensive names
    - No, haven't experienced any
94. Where have you experienced online harassment?
    - Facebook
    - Twitter
    - Online dating sites
    - Online games
95. Whether you have responded to online harassments that you have experienced?
    - Yes, responded to them
    - No, ignored them
96. Which of the following was your response to the online harassment you experienced
    - Unfriended or blocked the person
    - Confronted the person online
    - Reported the person responsible to the website or online server
    - Withdrew from an online forum
    - Deleted your social media account
97. Are you a personal member or have an account with the following social media sites?
    - Facebook
    - Gmail
    - Yahoo mail

- YouTube
- Instagram
- Viber
- Lazada
- Metrodeal
- Multiply

98. How often do you use social media?
    - Daily, +3 hours a day
    - Daily, +2 hours a day
    - Daily, less than an hour a day
    - A few days per week
    - Seldom
99. Those you have a social media account what is the extent of your trust in these sites
    - Gmail
    - Lazada
    - YouTube
    - Instagram
    - Facebook
    - Viber
    - Twitter
    - Yahoo mail
    - Metrodeal
    - Multiply

    Much trust – little trust – undecided
100. Do you know the privacy settings of the app you are using?
    - Yes
    - No
101. Have you checked the privacy settings of the app you are using?
    - Yes, have checked
    - No, have not checked
102. How often do you change the privacy settings of the app you are using?
    - Everyday
    - Several times a week
    - Once a week
    - 2-3 times a week
    - Once a month
    - Several times a year
    - Once a year
    - Never
103. Are you currently tracking any elected official, election candidate or other politician on a social networking site such as Facebook, Youtube, Multiply or Twitter?
    - Yes
    - No
104. Do you use social networking sites like Facebook, Youtube, Multiply or Twitter to post links to stories or political articles for others to read?

- Yes
- No

105. Do you use social networking sites like Facebook, Youtube, Multiply or Twitter to post your opinions or comments on political or social issues?
    - Yes
    - No
106. Are you currently tracking any artist or sports personality on a social networking site such as Facebook, Youtube, Multiply or Twitter?
    - Yes
    - No
107. Do you use social networking sites like Facebook, Youtube, Multiply or Twitter to post links to stories or articles about showbiz or sports for others to read?
    - Yes
    - No
108. Do you use social networking sites like Facebook, Youtube, Multiply or Twitter to post your ideas or comments on showbiz or sports issues?

European Commission

Survey 1: Special Eurobarometer 431

1. Please tell me how often you do each of the following activities online
   Every day/ Almost every day – Two or three times a week – About once a week – Two or three times a month – less often – Never – Don't know
   - Use an online social network, for instance to share pictures, videos, movies, etc.
   - Purchase goods or services online (e.g. travel & holiday, clothes, books, tickets, films, music, software, food)
   - Use instant messaging, chat websites
   - Use peer-to-peer software or sites to exchange movies, music, etc.
   - Make or receive phone calls or video calls over the Internet
   - Use online banking
   - Play online games
2. Please tell me whether you agree or disagree with each of the following statements
   Totally agree – tend to agree – tend to disagree – totally disagree – not applicable – Don't know
   - The (NATIONALITY) Government asks you for more and more personal information
   - You feel you have to provide personal information online
   - There is no alternative than to provide personal information if you want to obtain products or services
   - Providing personal information is not a big issue for you
   - Providing personal information is an increasing part of modern life
   - You don't mind providing personal information in return for free services online (e.g. free email address)
3. When online (using online social networks or mobile applications, making online purchases, etc.), you are sometimes asked to provide personal information. What are the main reasons why you provide personal information online?
   - To access the service
   - To save time at the next visit
   - To receive money or price reductions
   - To benefit from personalised commercial offers
   - To get a service for free
   - To obtain a service adapted to your needs
   - To connect with others
   - To make a payment online
   - To have your purchase delivered
   - Other (specify)
   - You never provide personal information online
   - Don't know
4. How much control do you feel you have over the information you provide online, e.g. the ability to correct, change or delete this information?
   - Complete control
   - Partial control

- No control at all
- It depends on the website or application (specify)
- Don’t know

5. How concerned are you about not having complete control over the information you provide online? Would you say you are…?
   - Very concerned
   - Fairly concerned
   - Not very concerned
   - Not at all concerned
   - Don’t know
6. Have you ever heard of recent revelations about government agencies collecting personal data on a large scale for the purpose of national security?
   - Yes
   - No
   - Don’t know
7. Would you say these recent revelations have had an impact on the trust in how your online personal data is used?
   - Yes, a positive impact
   - Yes, a negative impact
   - No , no impact at all
   - Don’t know
8. If you use the internet, I will read out a list of potential risks for your personal information. According to you, what are the most serious risks of providing personal information online?
   - Your information being used without your knowledge
   - Your information being shared with third parties (companies or government agencies) without your consent
   - Your information being used to send you unwanted commercial offers
   - Your views and behaviours being misunderstood
   - Your online identity being used for fraudulent purposes
   - Your personal safety being at risk
   - Becoming a victim of fraud
   - Becoming the victim of discrimination (e.g. in job recruitment, being charged higher prices, not being able to access a service)
   - Your reputation being damaged
   - Your information being used in different contexts from those in which you provided it
   - Your personal information being stolen
   - Your personal information being lost
   - Other (specify)
   - None (specify)
   - You never provide personal information online (specify)
   - Don’t know

A personal profile on an online social network usually includes information such as your age, interests, a photo and an "about me" section. Profile visibility, i.e. who can see your information

and interact with you, can, in some cases, be personalised by managing the privacy settings offered by the site.

9. Have you ever tried to change the privacy settings of your personal profile from the default settings on an online social network?
   - Yes
   - No
   - Don't know
10. How easy or difficult did you find it to change the privacy settings of your personal profile?
   - Very easy
   - Fairly easy
   - Fairly difficult
   - Very difficult
   - Don't know
11. Why have you not tried to change these privacy settings?
   - You did not know that you could change the settings
   - You do not know how to change these settings
   - You trust the sites to set appropriate privacy settings
   - You are not worried about having personal data on an online social network
   - You have not had the time to look at the available options
   - Other (specify)
   - Don't know
12. Who do you think should make sure the information you provide online is collected, stored and exchanged safely? Firstly?
13. And secondly?
   - You – as you need to take care of your information
   - Online companies – as they used to ensure they process your information safely
   - Public authorities – as they need to ensure that citizens' data are protected
   - Other (specify)
   - You never provide personal information online (specify)
   - Don't know
14. Nowadays, many of our everyday activities are recorded in different ways, such as through cameras, payment cards, websites, etc. How concerned or not are you about that?
   - On the Internet (browsing, downloading files, accessing online content)
   - In a public space (street, metro, airport, etc.)
   - In a private space (restaurant, bar, club, office, etc.)
   - Via mobile phone or use of mobile applications (listening in on your calls, geo-location)
   - Via payment cards (your location and spending habits)
   - Via store or loyalty cards (your preferences and patterns of consumption, etc.)
15. When you are asked to provide personal information online, would you say that you are usually informed about the conditions of the data collection and the further uses of your data?
   - Always

- Sometimes
- Rarely
- Never
- You are never asked to provide personal information online
- Don’t know

16. On the Internet, privacy statements explain how the personal information you provide will be used and who will have access to it. Thinking about privacy statements on the Internet, which of the following sentences best describes what you usually do?
    - You read them fully
    - You read them partially
    - You do not read them at all
    - Don’t know
17. What are the reasons why you usually do not read or read only partially the privacy statements?
    - You think the websites will not honour them anyway
    - You believe that the law will protect you in any case
    - You don’t know where to find them
    - You don’t think it is important to read them
    - You find them too long to read
    - You find them unclear, too difficult to understand
    - It is sufficient for you to see that websites have a privacy policy
    - Other (specify)
    - Don’t know
18. As you may know, some online companies are able to provide free services, such as search engines, free e-mail accounts, etc., thanks to the income they receive from advertisers trying to reach users on their websites. How comfortable are you with the fact that those websites use information about your online activity to tailor advertisements or content to your hobbies and interests?
    - Very comfortable
    - Fairly comfortable
    - Fairly uncomfortable
    - Very comfortable
    - Don’t know
19. Should your explicit approval be required before any kind of personal information is collected and processed?
    - Yes, in all cases
    - Yes, in the case of personal information required online
    - Yes, in the case of sensitive information whether online or offline (e.g. health, religion, political beliefs, sexual preferences, etc.)
    - No
    - Don’t know
20. Different authorities (government departments, local authorities, agencies) and private companies collect and store personal information about you. To what extent do you trust the following authorities and private companies to protect your personal information? Totally trust – tend to trust – tend not to trust – do not trust at all – don’t know

- National public authorities (e.g. tax authorities, social security authorities)
- European institutions (European commission, European parliament, etc.)
- Banks and financial institutions
- Health and medical institutions
- Shops and stores
- Online businesses 9search engines, online social networks, e-mail services)
- Landline or mobile phone companies and internet services providers

21. Authorities and private companies holding information about you may sometimes use it for a different purpose than the one it was collected for, without informing you (e.g. for direct marketing, targeted online advertising, profiling). How concerned are you about this use of your information?
    - Very concerned
    - Fairly concerned
    - Not very concerned
    - Not at all concerned
    - Don't know
22. When you decide to change online service providers (e.g. an online social network or a cloud service provider), how important or not is it for you to be able to transfer personal information that was stored and collected by the old provider to the new one?
    - Very important
    - Fairly important
    - Not very important
    - Not at all important
    - Don't know
23. Would you want to be informed if information that is held about you is lost or stolen?
    - Yes
    - No
    - Don't know
24. Who do you think should inform you if information that is held about you is lost or stolen?
    - The authority or private company handling your data
    - The (Nationality) data protection authority
    - The data protection authority of the country where the authority or private company is established
    - A court
    - An independent organisation for the protection of data rights
    - Other (specify)
    - Don't know
25. How important or not is it for you to have the same rights and protections over your personal information regardless of the country in which the authority or private company offering the service is established?
    - Very important
    - Fairly important
    - Not very important
    - Not at all important
    - Don't know

26. In your opinion, the enforcement of the rules on personal data protection should be dealt with at…?
    - European level
    - National level
    - Regional or local level
    - Don’t know
27. Have you heard about a public authority in (OUR COUNTRY) responsible for protecting your rights regarding your personal data?
    - Yes
    - No
    - Don’t know
28. If you experienced a problem concerning the protection of your personal data, to whom would you prefer to send a complaint?
    - The authority or private company handling your data
    - The (Nationality) data protection authority
    - The data protection authority of the country where the authority or private company is established
    - A court
    - An independent organisation for the protection of data rights
    - The EU institutions and bodies
    - Other (specify)
    - Don’t know
29. Which data would you be most concerned about, if it was lost or stolen?
    - Data stored on your mobile phone or tablet
    - Data stored online or in the cloud
    - Data stored on your computer
    - Other (specify)
    - Don’t know

Survey 2: EU Special Eurobarometer 464a

1. Could you tell me if…?
   - You use the internet at home, in your home
   - You use the internet on your place of work
   - You use the internet on your mobile device (laptop, smartphone, tablet, etc.)
   - You use the internet somewhere else (school, university, cyber-café, etc.)

   Every day or almost every day – two or three times a week – about once a week – Two or three times a month – Less often – Never – No internet access
2. What devices do you use to access the Internet?
   - Computer (desktop, laptop, netbook)
   - Tablet
   - Smartphone
   - TV
   - Other (specify)
   - Don't know
3. Which of the following activities do you do online?
   - Online banking
   - Buying goods or services (holidays, books, music, etc.)
   - Selling goods or services
   - Sending or receiving email
   - Reading news
   - Playing games
   - Watching TV
   - Other (specify)
   - Don't know
4. What concerns do you have, if any, about using the Internet for things like online banking or buying things online?
   - Online banking
   - Buying goods or services (holidays, books, music, etc.)
   - Selling goods or services
   - Sending or receiving email
   - Reading news
   - Playing games
   - Watching TV
   - Other (specify)
   - Don't know
5. Thinking about online harassment (e.g. cyber bullying or blackmailing), what, if anything, is done in your household to protect children under 16 years old while they are online?
   - Monitor child's internet usage
   - Adjust security settings on browser etc. for use by child
   - Limit time spent by child online
   - Talk to child about risks on internet
   - You would like to do something, but you do not know how
   - Other

- Nothing
- Not applicable
- Don’t know

6. How well informed do you feel about the risks of cybercrime?
   - Very well informed
   - Fairly well informed
   - Not very well informed
   - Not at all informed
   - Don’t know
7. Cybercrimes can include many different types of criminal activity. How concerned are you personally about experiencing or being a victim of the following situations?
   Very concerned – fairly concerned – not very concerned – not at all concerned – Don’t know
   - Identify theft (somebody stealing your personal data and impersonating you)
   - Receiving fraudulent emails or phone calls asking for your personal details (including access to your computer, logins, banking or payment information)
   - Online fraud where goods purchased are not delivered, are counterfeit or not as advertised
   - Accidentally encountering child pornography online
   - Accidentally encountering material which promotes racial hatred or religious extremism
   - Not being able to access online services like banking or public services because of cyber attacks
   - Your social network account or email being hacked
   - Being a victim of bank card or online banking fraud
   - Being asked for a payment in return for getting back control of your device
   - Discovering malicious software (viruses, etc.) on your device
8. And how often have you experienced or been a victim of the following situations?
   Often – occasionally – never – don’t know
   - Identify theft (somebody stealing your personal data and impersonating you)
   - Receiving fraudulent emails or phone calls asking for your personal details (including access to your computer, logins, banking or payment information)
   - Online fraud where goods purchased are not delivered, are counterfeit or not as advertised
   - Accidentally encountering child pornography online
   - Accidentally encountering material which promotes racial hatred or religious extremism
   - Not being able to access online services like banking or public services because of cyber attacks
   - Your social network account or email being hacked
   - Being a victim of bank card or online banking fraud
   - Being asked for a payment in return for getting back control of your device
   - Discovering malicious software (viruses, etc.) on your device
9. If you experienced or were a victim of the following situations, who would you contact?

Police – website/vendor – your internet service provider – consumer protection organisation – other – no one – don't know

- Identify theft (somebody stealing your personal data and impersonating you)
- Receiving fraudulent emails or phone calls asking for your personal details (including access to your computer, logins, banking or payment information)
- Online fraud where goods purchased are not delivered, are counterfeit or not as advertised
- Accidentally encountering child pornography online
- Accidentally encountering material which promotes racial hatred or religious extremism
- Not being able to access online services like banking or public services because of cyber attacks
- Your social network account or email being hacked
- Being a victim of bank card or online banking fraud
- Being asked for a payment in return for getting back control of your device
- Discovering malicious software (viruses, etc.) on your device

10. Could you please tell me to what extent you agree or disagree with each of the following statements?

    Totally agree – tend to agree – tend to disagree – totally disagree – don't know

    - You are concerned that your online personal information is not kept secure by websites
    - You are concerned that your online personal information is not kept secure by public authorities
    - You avoid disclosing personal information online
    - You believe the risk of becoming a victim of cybercrime is increasing
    - You are able to protect yourself sufficiently against cybercrime, e.g. by using antivirus software

11. Have you changed your password to access your account(s) for any of the following online services during the last 12 months?

    - Email
    - Online social networks
    - Shopping websites
    - Online banking
    - Online games
    - Public services websites
    - Other (specify)
    - None (specify)
    - Don't know

Survey 1: IAPP Governance and Operations Survey 2018

A. Company Information

A1. In this first section, we'll ask about your role and about the company you work for. First, which of the following BEST describes the sector of your current position? **IF TERMINATE, INCLUDE NOTE THANKING FOR TIME AND EXPLAINING THAT THIS PARTICULAR STUDY FOCUSES ON IN-HOUSE PRIVACY PROFESSIONALS**

- ❑ **Private-sector, in-house privacy professional**: You work on the internal privacy needs of a privately held company.
- ❑ **Government sector, in-house privacy professional**: You work on the internal privacy needs of a government agency.
- ❑ **Non-profit sector, in-house privacy professional:** You work on the internal privacy needs of a non-profit institution.
- ❑ **Education sector, in-house privacy professional:** You work on the internal privacy needs of an educational institution.
- ❑ **Any sector, in-house IT professional**: You work on the internal information-technology needs of your company.
- ❑ **Researcher or academic**: You work as a researcher, professor or writer on the topic of privacy (other than working in the educational sector). **TERMINATE**
- ❑ **Regulator**: You work for an agency that monitors and enforces compliance with privacy regulations. **TERMINATE**
- ❑ **External privacy advisor**: You work as a privacy consultant, attorney, barrister, solicitor or auditor on the privacy needs of other companies. **TERMINATE**
- ❑ **Vendor**: You work for a company that sells privacy-related products or services. **TERMINATE**
- ❑ **Privacy advocate**: You raise public awareness about privacy, work toward open debate on privacy risks and lobby for privacy regulations. **TERMINATE**

- ❑ Other

_____

TERMINATE BUT KEEP RECORD OF VERBATIMS

A1a. Which sector listed below best describes how your company would be classified?

- ❑ Consulting services
- ❑ Legal services
- ❑ Chemical and agriculture
- ❑ Consumer products
- ❑ Energy and utilities
- ❑ Financial services and insurance
- ❑ Government
- ❑ Healthcare and pharmaceutical
- ❑ Manufacturing
- ❑ Media and communication

- ❑ Retail
- ❑ Hotels, restaurants, leisure
- ❑ Transportation
- ❑ Technology and telecommunications
- ❑ Other (PLEASE SPECIFY)

A1b. Does your company primarily serve:
Select one response only.

- ❑ Other businesses (B2B)
- ❑ Consumers (B2C)
- ❑ Businesses and consumers (B2B and B2C)

A2. Keeping in mind this survey is confidential and your individual information will not be shared, please tell us (as accurately as you can) your company's annual revenue.
Your best estimate is fine.

_____

A3. What is the total number of employees in your company (full-time and part-time)? We are looking for the total number for your entire company. If you work in a subsidiary of another corporation, please answer for the subsidiary only.
Your best estimate is fine.

_____

A4. What is the primary location of your company's **headquarters**?
Select one response only from list below.

A5. In what region and country are **you** currently based?
Select one response only from list below.

English-Speaking Countries
- ❑ United States
- ❑ Canada
- ❑ U.K.
- ❑ Australia
- ❑ New Zealand

Latin America:
- ❑ Argentina
- ❑ Brazil
- ❑ Chile
- ❑ Colombia
- ❑ Ecuador
- ❑ Guatamale
- ❑ Mexico
- ❑ Peru

- ❑ Venezuela
- ❑ Other Latin America **PLEASE SPECIFY**

European Union
- ❑ Austria
- ❑ Belgium
- ❑ Finland
- ❑ France
- ❑ Germany
- ❑ Greece
- ❑ Ireland
- ❑ Italy
- ❑ Netherlands
- ❑ Portugal
- ❑ Slovakia
- ❑ Slovenia
- ❑ Spain
- ❑ Other EU **PLEASE SPECIFY**

Non-EU Europe
- ❑ Albania
- ❑ Armenia
- ❑ Belarus
- ❑ Iceland
- ❑ Kosovo
- ❑ Norway
- ❑ Russian Federation
- ❑ Switzerland
- ❑ Turkey
- ❑ Ukraine
- ❑ Other non-EU Europe **PLEASE SPECIFY**

Africa
- ❑ Algeria
- ❑ Angola
- ❑ Democratic Republic of Congo
- ❑ Egypt
- ❑ Ethiopia
- ❑ Ghana
- ❑ Kenya
- ❑ Madagascar
- ❑ Morocco
- ❑ Mozambique
- ❑ Nigeria
- ❑ South Africa
- ❑ Sudan
- ❑ Uganda
- ❑ Other Africa **PLEASE SPECIFY**

Middle East
- ❑ Bahrain
- ❑ Egypt

- ❑ Israel
- ❑ Jordan
- ❑ Kuwait
- ❑ Quatar
- ❑ Saudi Arabia
- ❑ UAR
- ❑ Yemen
- ❑ Other Middle East **PLEASE SPECIFY**

Asia
- ❑ Bangladesh
- ❑ China
- ❑ India
- ❑ Indonesia
- ❑ Japan
- ❑ Myanmar
- ❑ Pakistan
- ❑ Philippines
- ❑ Singapore
- ❑ South Korea
- ❑ Thailand
- ❑ Vietnam
- ❑ Other Asia **PLEASE SPECIFY**

- ❑ Other **country: PLEASE SPECIFY**

A6. Do you collect personal data from data subjects in any of the following regions and countries?
Please select all that apply from list below.

English-Speaking Countries
- ❑ United States
- ❑ Canada
- ❑ U.K.
- ❑ Australia/New Zealand

Latin America
- ❑ Any Latin American country

European Union
- ❑ France
- ❑ Germany
- ❑ Ireland
- ❑ The Netherlands
- ❑ Italy
- ❑ Spain
- ❑ Other EU country

Non-EU Europe
- ❑ Any non-EU Europe country

Africa
- ❑ Any African country

Middle East
- ❑ Any Middle Eastern country

Asia
- ❑ China
- ❑ India
- ❑ Singapore
- ❑ Hong Kong
- ❑ Other Asian country

A7. In addition to your **headquarters** location, does your company also have **regional offices** in any of the countries in which you do business?

- ❑ Yes, has regional offices
- ❑ No, does not

D. Privacy Responsibilities

D1. About what percent of your own work at your company is made up of privacy responsibilities?

SLIDER: 0-100%

D2. Which of the following levels best describes your position in your company? ***Please select one response only. Please consider the title "Director" to refer to a position between a Manager and a Vice President. It does NOT denote membership in the Board of Directors. Please consider "General Counsel" to be the highest-ranking lawyer in the company.***

- ❑ C-Suite
- ❑ Executive Vice President
- ❑ Senior Vice President
- ❑ Vice President
- ❑ General Counsel
- ❑ Director
- ❑ Assistant or Associate counsel
- ❑ Manager
- ❑ Supervisor
- ❑ Solutions Architect
- ❑ Coordinator
- ❑ Individual Contributor
- ❑ Analyst
- ❑ Other (specify) _____

D2a. What is your exact title? _____

D3. Which of the following functions best describe the areas you **regularly** work with at your company? ***Select all that apply.***

- ❑ Corporate Ethics
- ❑ Consulting
- ❑ Finance and Accounting
- ❑ Government Affairs
- ❑ Human Resources
- ❑ Information Security
- ❑ Information Technology
- ❑ Internal Audit
- ❑ Legal
- ❑ Marketing
- ❑ Physical Security
- ❑ Procurement
- ❑ Public Relations
- ❑ Records Management
- ❑ Regulatory Compliance
- ❑ Risk Management
- ❑ Research and Development
- ❑ Other

D4. Which of the following is the privacy **team generally** responsible for accomplishing on an annual basis, whether or not you personally are involved? ***Please check all that apply.***

- ❑ Development and training for privacy staff
- ❑ Company privacy-related awareness and training
- ❑ Privacy-related communications
- ❑ Privacy-related monitoring
- ❑ Privacy audits
- ❑ Privacy policies, procedures and governance
- ❑ Data inventory and mapping
- ❑ Privacy-related subscriptions and publications
- ❑ Preparation for General Data Protection Regulation (GDPR)
- ❑ Assuring proper cross-border data transfer
- ❑ Acquiring and/or using privacy-enhancing software
- ❑ Incident response
- ❑ Privacy-related investigations
- ❑ Privacy-related legal counsel (internal)
- ❑ Privacy-related vendor management
- ❑ Privacy-related web certification and seals
- ❑ Redress and consumer outreach
- ❑ Guiding the design and implementation of privacy controls
- ❑ Participating in data related internal committees
- ❑ Addressing privacy by design in product development
- ❑ Performing Privacy Impact Assessments (or Data Protection Impact Assessments)
- ❑ Addressing privacy issues with existing products and services

- ❑ Ethical decision-making around data use
- ❑ None of the above **[EXCLUSIVE]**

D5. Next, for employees who are **OUTSIDE the privacy team** generally but **have privacy responsibilities,** which of the following are **they** rsponsible for accomplishing on an annual basis, whether or not you personally are involved? ***Please check all that apply.***

- ❑ Development and training for privacy staff
- ❑ Company privacy-related awareness and training
- ❑ Privacy-related communications
- ❑ Privacy-related monitoring
- ❑ Privacy audits
- ❑ Privacy policies, procedures and governance
- ❑ Data inventory and mapping
- ❑ Privacy-related subscriptions and publications
- ❑ Preparation for General Data Protection Regulation (GDPR)
- ❑ Assuring proper cross-border data transfer
- ❑ Acquiring and/or using privacy-enhancing software
- ❑ Incident response
- ❑ Privacy-related investigations
- ❑ Privacy-related legal counsel (internal)
- ❑ Privacy-related vendor management
- ❑ Privacy-related web certification and seals
- ❑ Redress and consumer outreach
- ❑ Guiding the design and implementation of privacy controls
- ❑ Participating in data related internal committees
- ❑ Addressing privacy by design in product development
- ❑ Performing Privacy Impact Assessments (or Data Protection Impact Assessments)
- ❑ Addressing privacy issues with existing products and services
- ❑ Ethical decision-making around data use
- ❑ None of the above **[EXCLUSIVE]**

E. Program Maturity and Goals

ASK E SERIES ONLY IF DIRECTOR LEVEL OR HIGHER IN D2

E. These next questions are about your company's privacy program generally.

E1. First, please select the maturity stage of your company's privacy program. ***Select the one that in your opinion best describes the activities associated with your company's current privacy office or initiatives.***

- ❑ **Early Stage** –Privacy program is just starting to be established as a unit within the company
- ❑ **Middle Stage** – Privacy program is in existence and is starting to launch key initiatives but is not yet firmly established with key decision-makers
- ❑ **Mature Stage** – Privacy program is well-established and well-understood throughout the company

E2. For how many years has your company had a dedicated privacy program? ***Your best estimate is fine.***

_____

E3. Please rank the following in terms of their priority for your company's privacy program. Put a 1 for the most important priority, a 2 for the second most important priority, and so on, until the 9th or least important priority.

RANDOMIZE LIST

____ Enhance marketplace reputation and brand
____ Regulatory and legal compliance (beyond the EU General Data Protection Regulation)
____ Compliance with the EU General Data Protection Regulation
____ Safeguard data against attacks and threats
____ Maintain or enhance the value of information assets
____ Reduce the risk of employee and consumer lawsuits
_____ Meet the expectations of business clients and partners
_____ Increase revenues
_____ To be a good corporate citizen

F. Structure and Budget

ASK F SERIES ONLY IF DIRECTOR LEVEL OR HIGHER IN D2

PROGRAM SIZE AND BUDGET

F1. How many of the employees in your company are:

FULL TIME	
Dedicated **full-time** to privacy and working in your company's **privacy program**	
Dedicated **full-time** to privacy but working in **internal service centers** like HR, IT, and creative services	
Dedicated **full-time** to privacy but working in **revenue-related business units** like marketing, sales, and product development	
PART TIME	
Dedicated **part time** to privacy and working in your company's **privacy program**	
Dedicated **part time** to privacy but working in **internal service centers** like HR, IT, and creative services	
Dedicated **part time** to privacy but working in **revenue-related business units** like marketing, sales, and product development	

F2. In the coming year, do you expect the number of employees in each of these categories to increase, decrease, or stay the same?'

- If staying the same, please click the option under "Stay the same."
- If increase, please enter your estimate of the percentage you expect the overall number of employees to increase under "Increase."
- If decrease, please enter your estimate of the percentage you expect the overall number of employees to decrease under "decrease."

[PROGRAMMING NOTE: ALLOW ONE RESPONSE PER ROW]

	Increase/%	Decrease/%	Stay the same
FULL TIME			
Dedicated **full-time** to privacy and working in your company's **privacy program**			
Dedicated **full-time** to privacy but working in **internal service centers** like HR, IT, and creative services			
Dedicated **full-time** to privacy but working in **revenue-related business units** like marketing, sales, and product development			
PART TIME			
Dedicated **part time** to privacy and working in your company's **privacy program**			
Dedicated **part time** to privacy but working in **internal service centers** like HR, IT, and creative services			
Dedicated **part time** to privacy but working in **revernue-related business units** like marketing, sales, and product development			

F3. What percent of your company's total privacy spend is allocated to each of the following components?

Your best estimate is fine, but please make sure the total equals 100 percent.

___% Salary and travel
___% Professional development (e.g., conferences and training)

___% Outside counsel
___% Consulting services
___% Technology and tools
___% Associations or government relations
___% Other _____

F4. And what is the total privacy spend for your company in each of the following categories? ***(Please state in [A4 CURRENCY])***

$_____Budget controlled by the privacy team, not including salaries and benefits
$_____Salaries and benefits of the privacy team
$_____Spend on privacy-related activities outside of the privacy team, not included in the privacy team's budget (for example, privacy technologies deployed by HR or IT)

F4a. Use the following scale to tell us how much flexibility your company has with its privacy spending through the year. **Select one response only**

←Strict adherence to budget/no flexibility				**Need special authorization to go outside budget**					**Can go beyond budget as needed →**	

❑ We have no fixed privacy budget for the year

F5. In the next 12 months, you expect that the total amount your company spends on privacy, including salaries and benefits, will …

❑ Increase
❑ Decrease
❑ Stay the same
❑ Cannot tell

F6. Overall, would you say that your company's privacy budget is …

❑ More than sufficient to meet your privacy obligations
❑ Sufficient to meet your privacy obligations
❑ Somewhat less than sufficient to meet your privacy obligations
❑ Much less than sufficient to meet your privacy obligations

ASK F11 IF HAVE REGIONAL OFFICES IN A7

F11. Is the privacy program of your company geographically located…

❑ At headquarters only
❑ Mostly at headquarters with some members disbursed across regional offices
❑ Mostly spread across regional offices with some at headquarters
❑ Across our regional offices with none at headquarters

F12. In which department within your company is the privacy **TEAM** located?

- ❑ Corporate Ethics
- ❑ Finance and Accounting
- ❑ Government Affairs
- ❑ Human Resources
- ❑ Information Security
- ❑ Information Technology
- ❑ Internal Audit
- ❑ Marketing
- ❑ Physical Security
- ❑ Procurement
- ❑ Public Relations
- ❑ Records Management
- ❑ Regulatory Compliance
- ❑ Legal
- ❑ Other **PLEASE SPECIFY**

F13. In which department are you personally located?

- ❑ Corporate Ethics
- ❑ Finance and Accounting
- ❑ Government Affairs
- ❑ Human Resources
- ❑ Information Security
- ❑ Information Technology
- ❑ Internal Audit
- ❑ Marketing
- ❑ Physical Security
- ❑ Procurement
- ❑ Public Relations
- ❑ Records Management
- ❑ Regulatory Compliance
- ❑ Legal
- ❑ Other **PLEASE SPECIFY**

F14. Will Brexit affect the organization of your privacy team?

- ❑ Yes
- ❑ No
- ❑ Do not know

ASK F15-F17 IF YES IN F14

F15. In what ways will Brexit affect the organization of your privacy team? **Select all that apply**

- ❑ Privacy leadership will be relocated to a new EU country
- ❑ New, UK-specific privacy team will be created
- ❑ Will have to establish a new lead supervisory authority
- ❑ Will have to find new lead authority for BCRs
- ❑ Other **PLEASE SPECIFY**

ASK IF PRIVACY LEADERSHIP WILL BE RELOCATED IN F15

F16. In which new country will you relocate your privacy leadership?

OPEN END

- ❑ Do not know

ASK IF PRIVACY LEADERSHIP WILL BE RELOCATED IN F15

F17. What factors will go into the decision as to which country to relocate the privacy team to? **Select all that apply**

- ❑ Relationship with the supervisory authority
- ❑ The country's data protection laws, including derogations from the GDPR
- ❑ Enforcement history of the supervisory authority
- ❑ Only option, given corporate locations
- ❑ Other **PLEASE SPECIFY**

F18. Are **you** the company's Privacy Leader, or is that someone else? By "Privacy Leader," we mean the person in the company—whatever their specific title—who is ultimately responsible for managing and overseeing your company's privacy policies and initiatives.

- ❑ I am the Privacy Leader
- ❑ Someone else is the Privacy Leader

ASK F21 IF SOMEONE ELSE IN F18

F21. What is the exact title of the Privacy Leader in your company?

OPEN END

ASK ALL

F22. How does the position of the Privacy Leader compare with that of your company's chief information security officer or the highest level information security person in the company, if any? The Privacy Leader is …

- ❑ The same person as the chief information security officer
- ❑ A more junior position than the chief information security officer

- ❑ An equivalent level to the chief information security officer
- ❑ A more senior position than the chief information security officer
- ❑ We do not have a chief information security officer

F23. How does the position of the Privacy Leader compare with that of your company's chief privacy counsel, if any? The Privacy Leader is …

- ❑ The same person as the chief privacy counsel
- ❑ A more junior position than the chief privacy counsel
- ❑ An equivalent level to the chief privacy counsel
- ❑ A more senior position than the chief privacy counsel
- ❑ We do not have a chief privacy counsel

F24. Does the Privacy Leader have responsibilities other than privacy?

- ❑ Yes
- ❑ No

F25. To whom in your company does the Privacy Leader report? Just write in the positions or titles.

OPEN END

F26. Does the privacy leader report to your company's board of directors?

- ❑ Yes
- ❑ No
- ❑ Don't know

F28. Are **you** the company's "data protection officer," or is that someone else? By "data protection officer," we mean the person in the company—holding that specific title— responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements or any other law that requires the role of the DPO.

- ❑ I am the data protection officer
- ❑ Someone else is the data protection officer
- ❑ We do not have a data protection officer

IF NO DATA PROTECTION OFFICER IN F28, SKIP TO QF37

F29. What is the exact title of the data protection officer in your company?

OPEN END

F30. Does your company have only one data protection officer responsible for overseeing data protection strategy across the company? Or does it have more than one?

- ❑ One data protection officer
- ❑ More than one data protection officer **PLEASE SPECIFY HOW MANY YOU HAVE**

F31. How does the position of the Privacy Leader compare with that of your company's data protection officer, if any? The Privacy Leader is …

- ❑ The same person as the data protection officer
- ❑ A more junior position than the data protection officer
- ❑ An equivalent level to the data protection officer
- ❑ A more senior position than the data protection officer

ASK IF PRIVACY LEADER IS NOT THE SAME PERSON AS DPO IN F31

F32. To whom in your company does the data protection officer report? *Please select as many as needed*

- ❑ The Privacy Leader
- ❑ Other positions **PLEASE SPECIFY**

F34. Does your company have a separate, dedicated staff reporting to the data protection officer?

- ❑ Yes, dedicated staff reports to data protection officer
- ❑ A few people report to the data protection officer, but not a full staff
- ❑ No, the data protection officer does not have any reports or staff

- ❑ Other positions **PLEASE SPECIFY**

F35. Which of the following best describes the MAIN reason why your company has a data protection officer? **Select one response only**

- ❑ We're required to by law—otherwise we wouldn't have one
- ❑ It serves a valuable purpose in our company

F36. Once GDPR duties are completed in your company, will you continue to have a data protection officer?

- ❑ Yes, and it will be the same person who has that position today
- ❑ Yes, but it will be a different person
- ❑ No, we'll no longer have a data protection officer

ASK F37 IF HAVE NO DPO IN F28

F37. What is the main reason you do not have a data protection officer in your company? **Select one response only**

- ❑ We are not subject to GDPR or believe the DPO requirements do not apply to us

- ❑ We should have a DPO under the GDPR, but just haven't gotten around to it yet, and will have one in the future
- ❑ We are not sure if we are required to have a DPO and we are concerned about having a position with the legal responsibilities required of a DPO
- ❑ Other reason **PLEASE SPECIFY**

F38. Aside from who does the actual reporting, are privacy-related matters at your company reported to the board of directors or the board level generally?

- ❑ Yes
- ❑ No
- ❑ Don't know

ASK F39-F43 IF YES IN F38

F39. What privacy topics are reported at the board level?
Please check all that apply.

- ❑ Privacy program key performance indicators (KPIs) (number of subject access requests handled, number of internal privacy incidents identified, etc.)
- ❑ Status of compliance with GDPR
- ❑ Information regarding certifications and attestations (i.e., SOC2, ISO)
- ❑ Privacy litigation
- ❑ Data breaches
- ❑ Number of privacy complaints
- ❑ Privacy compliance developments (e.g., BCR or Model Clause approvals)
- ❑ Progress on privacy initiatives
- ❑ Privacy budget details
- ❑ Specific incidents
- ❑ Questions of data ethics
- ❑ Other (please specify) _____

G. Cooperation

G5. In a general sense, for ongoing activities within your company that may involve privacy, representatives of the privacy program are involved …
Please check all that apply.

- ❑ From the outset
- ❑ On an ongoing basis throughout the activity
- ❑ At specific intervals throughout the activity
- ❑ At the end of the activity
- ❑ Only when called upon and as needed

G6. Now thinking strictly about new projects or initiatives established by your company that may involve privacy, representatives of the privacy program are involved …

Please check all that apply.

- ❑ At the budget stage
- ❑ At development stage
- ❑ When ready for rollout
- ❑ Only when needed

J. GDPR Section

J1. Does your company transfer personal information from the European Union and/or those countries in the European Economic Area (together: “EU”) to another country outside of the EU?

- ❑ Yes
- ❑ No
- ❑ Do not know

J2. [if yes to above]What mechanism does your company use to transmit data outside the EU? ***Check all that apply***

- ❑ Binding Corporate Rules (BCR)
- ❑ Privacy Shield
- ❑ Standard Contractual Clauses
- ❑ Consent
- ❑ Other statutory derogations, such as fulfillment of contract
- ❑ Certification or seal framework to be determined under GDPR
- ❑ Adherance to a code of conduct
- ❑ Adequacy
- ❑ None

ASK J3 IF BCR SELECTED IN J2

J3. When do you expect your BCR application to be approved?

- ❑ Our BCR application is already approved
- ❑ Within a year
- ❑ Within 1-3 years
- ❑ More than three years
- ❑ Do not know

J4. Do you offer goods or services to people residing in the European Union, even if there is no cost for acquiring those goods or services?

- ❑ Yes
- ❑ No
- ❑ Do not know

J5. Do you feel your company falls under the jurisdiction of the EU’s General Data Protection Regulation?

- ❑ Yes
- ❑ No
- ❑ Do not know

IF NO OR DO NOT KNOW TO GDPR IN J5, SKIP TO K1

J6. Does your company have to comply with both the GDPR and your national data protection and cybersecurity legal framework?

- ❑ Yes
- ❑ No

ASK IF YES IN J6

J7. How concerned are you that GDPR requirements could conflict with obligations set by national laws?

- ❑ Extremely concerned
- ❑ Very concerned
- ❑ Somewhat concerned
- ❑ Not very concrerned
- ❑ Not concerned at all

J8. Rate the following legal obligations of the General Data Protection Regulation in terms of how difficult they are for your company to comply. Use a scale of 0 to 10, where 0 means not difficult at all and 10 means extremely difficult.

- ❑ Understanding jurisdictional scope
- ❑ Fulfilling subject access requests
- ❑ Determing your lawful basis for processing
- ❑ Appointing a legal representative pursuant to Article 27
- ❑ Gathering explicit consent
- ❑ Breach notification requirements
- ❑ Restrictions on profiling
- ❑ Mandatory DPO requirement
- ❑ Cross border data transfer
- ❑ Right to be forgotten
- ❑ Data portability
- ❑ Conducting Data Protection Impact Assessments
- ❑ Understanding regulatory oversight

J9. What, if anything, has your company done to prepare for the GDPR? **PLEASE SELECT ALL THAT APPLY**

- ❑ Appoint a DPO
- ❑ Appoint multiple DPOs
- ❑ Invest in training
- ❑ Invest in technology
- ❑ Certify employees
- ❑ Create new relationship with outside counsel
- ❑ Create new relationship with consultancies
- ❑ Create new relationship with regulators
- ❑ Increase privacy budget
- ❑ Increase privacy staff
- ❑ Create new reporting structure
- ❑ Create new accountability framework
- ❑ Put in place new data transfer mechanism
- ❑ Cease to do business with persons in the EU
- ❑ Appoint a representative pursuant to Article 27
- ❑ Nothing [EXCLUSIVE]

J10. Has your privacy team's reporting structure changed in the last year as part of GDPR compliance efforts (for example, changes in whom people report to)?

- ❑ Yes
- ❑ No, but we're planning to change
- ❑ No, and we're not planning to change

J11. Have you elevated the position of privacy leader in the last year due to GDPR compliance efforts?

- ❑ Yes
- ❑ No, but we're planning to
- ❑ No, and we're not planning to

J11. Has reporting of privacy matters to the board of directors changed in the last year as part of GDPR compliance efforts?

- ❑ Yes
- ❑ No, but we're planning to change
- ❑ No, and we're not planning to change

J12. How many additional employees has your company hired to assist with GPDR-related activities, if any? **IF NONE, JUST TYPE IN 0**

____ Additional full-time employees to assist with GDPR activities
____ Additional part-time employees to assist with GDPR activities

J13. Has your company adapted products and services to be GDPR compliant?

- ❑ Yes
- ❑ No

❑ Do not know

ASK IF YES IN J13

J14. How much have you spent (including salaries and benefits) to adapt these current products and services to be GDPR compliant? ***(Please state in [A4 CURRENCY])***

$_____ spending to adapt products and services to GDPR

J15. How much do you expect to further spend (including salaries and benefits) **to adapt products and services to be GDPR compliant**? ***(Please state in [A4 CURRENCY])***

$_____ additional spending to adapt products and services to GDPR

J16. In addition to spending to adapt products and services, about how much do you think you will spend (including salaries and benefits) in your budget to comply with GDPR, **not including spending to adapt specific products and services**? We're just looking for your best estimate. **IF NONE, JUST TYPE IN 0** ***(Please state in [A4 CURRENCY])***

$_____ additional spending because of GDPR (other than products and services)

ASK IF >0 IN J16

J17. About what percentage of that additional budget for GDPR compliance falls into each of these categories?

___% Attorneys (outside counsel)
___ % Consultants
___ % Technology solution(s)
___ % Training
___ % Staff

J18. All things considered, how would you rate your current level of GDPR compliance?

←**Not at all compliant**								**Completely compliant** →		

ASK J19 IF LESS THAN TOP RATING IN J18

J19. When you do you expect to be completely compliant with the GDPR?

❑ Within the next month
❑ Within the next 3 months
❑ Within the next 6 months
❑ By the end of 2018
❑ After 2018
❑ Never

J20. Which of the following tools will you use to support the data inventory and mapping many companies perform to meet the record of processing activities requirements of GDPR? **SELECT ALL THAT APPLY**

- ❑ Governance, risk management and compliance (GRC) software that we customize for our inventory/mapping purposes
- ❑ Data loss prevention (DLP) technology
- ❑ Commercial software tool designed specifically for data inventory/mapping.
- ❑ System developed internally
- ❑ Manually/informally with email, spreadsheets, and in-person communication
- ❑ Outsource data inventory/mapping to external consultants/law firms
- ❑ Don't know

J21. When it comes to GDPR compliance, does your company consider unstructured data to be within scope for any of the following? **Select all that apply**

- ❑ Data inventory and mapping
- ❑ Record keeping
- ❑ Satisfying data subject rights
- ❑ None of these

J22. Has your company undertaken efforts specificaly aimed at data deletion?

- ❑ Yes, specifically within the context of enforcing minimum necessary retention
- ❑ Yes, specifically for satisfying data subject requests for deletion
- ❑ Yes, both for data subject requests and for minimum necessary retention
- ❑ No, we haven't undertaken data deletion efforts, but we're planning to delete data in response to subject requests and/or data retention requirements
- ❑ No, we haven't undertaken data deletion efforts, and we're not planning to

J23. How is your company addressing data subject requests, such as access, portability, right to be forgotten requests, or objections to processing?

- ❑ The process is automated
- ❑ The process is partially automated
- ❑ The process is entirely manual, but mature
- ❑ The process is entirely manual, and ad-hoc
- ❑ The process is still being designed
- ❑ We haven't taken steps to address these requests

J24. Per GDPR regulations, has your company identified a supervisory authority you consider to be your "lead supervisory authority"?

- ❑ Yes
- ❑ No
- ❑ Do not know

ASK J25-J26 IF YES IN J24

J25. In which country have you identified a lead supervisory authority? ***Select one response only***

- ❑ France
- ❑ Germany
- ❑ Ireland
- ❑ The Netherlands

- ❑ Italy
- ❑ Spain
- ❑ Other EU country

J26. What are the main reasons your company took steps to identify a specific lead supervisory authority? **Select all that apply**

- ❑ Had a prior relationship with the supervisory authority
- ❑ Derogations from the GDPR
- ❑ Enforcement history of the supervisory authority
- ❑ It was our only option given our corporate locations
- ❑ Any other reason **PLEASE SPECIFY**

J27. Pursuant to GDPR, has your company notified a supervisory authority of a high-risk processing activity?

- ❑ Yes
- ❑ No
- ❑ Do not know

J28. Pursuant to GDPR, has your company already notified any supervisory authorities of a data security breach?

- ❑ Yes
- ❑ No
- ❑ Do not know

J29. As a result of GDPR, how would you rate the risk to your organization of each of the following? Please use a scale from 1-5 where 1 means it is of no more risk than before GDPR, and 5 means it is a great deal more risk to your organization because of GDPR.

a. Employee related litigation
b. Consumer related litigation
c. Class action to seek injunctive relief
d. Class action to claim damages

H. Controller/Processor questions [ASK SECTION ONLY IF FALLS UNDER GDPR JURISDICTION IN J5]

H1. Does your company determine the purposes and means of processing personal data (ie., you are a “controller”)?

- ❑ Yes
- ❑ No
- ❑ Do not know

H2. Does your company process personal data on behalf of other companys (ie, you are a “processor”)?

- ❑ Yes
- ❑ No
- ❑ Do not know

H3. Does your company have other companies process personal data on your behalf (ie., you use "processors")?

- ❑ Yes
- ❑ No
- ❑ Do not know

H4. Have you changed your processors to any extent because of the GDPR?

- ❑ Yes
- ❑ No
- ❑ Do not know

H5. Have you brought processing in-house because of the GDPR?

- ❑ Yes
- ❑ No
- ❑ Do not know

H5a. Have you outsourced processing previously done in house because of the GDPR?

- ❑ Yes
- ❑ No
- ❑ Do not know

H6. Do you expect to change your processors because of the GDPR in the future?

- ❑ Yes
- ❑ No
- ❑ Do not know

H7. Have you lost business as a processor because of the GDPR?

- ❑ Yes
- ❑ No
- ❑ Do not know

ASK IF YES IN H3

H8. What steps do you take to ensure your processors are doing what they've committed to doing? **Select all that apply**

- ❑ Rely on assurances given in communications with the processors (email, phone conferences, etc.)
- ❑ Rely on assurances in the contract
- ❑ Require documention of third-party audit
- ❑ Require certification or proof of adherence to code of conduct
- ❑ Require completion of questionnaire(s)
- ❑ Conduct on-site audits ourselves
- ❑ Other steps **PLEASE SPECIFY**
- ❑ Nothing

H9. Are you in a business relationship where you consider yourself a “joint controller”?

- ❑ Yes
- ❑ No
- ❑ Do not know

H10. In your company, can non-lawyers, including potentially the DPO, negotiate data processing and joint controller agreements?

- ❑ Yes
- ❑ No
- ❑ Do not know

K. Additional Topics

ASK ALL

K1. When is your privacy program involved in the selection of new vendors? ***Please check all that apply.***

- ❑ Decisions to outsource
- ❑ Pre-contracting assessment
- ❑ Processor selection and contracting
- ❑ Ongoing processor due diligence or assessments
- ❑ Processor renewals
- ❑ Processor audits
- ❑ Processor termination
- ❑ Other (specify)
- ❑ Never

K2. Does your company have a vendor management program designed to ensure the privacy and/or security practices of vendors will not threaten the integrity of your company’s privacy standards?

- ❑ Yes
- ❑ No
- ❑ Do not know

ASK K3 IF YES IN K2

K3. Which, if any, third party audits or certifications does your company require from vendors? **Select all that apply**

- ❑ SOC2 Privacy
- ❑ APEC CBPRs
- ❑ The Japanese Privacy Mark System
- ❑ SOC2 HIPAA
- ❑ EU-U.S. Privacy Shield/Privacy Shield principles
- ❑ ISO 27001
- ❑ ISO 27002
- ❑ ISO 27018
- ❑ EuroPrise
- ❑ PCI
- ❑ CIPP/CIPM/CIPT

- ❑ CSA STAR
- ❑ An internal assessment that we've developed and vendors must "pass"
- ❑ TrustArc (formerly TRUSTe)
- ❑ We might require something, but I'm not sure
- ❑ Other (please specify)_____
- ❑ None

ASK ALL

K4. Will your company apply for Cross Border Privacy Rules (CBPR) to transfer data in the APEC region?

- ❑ Yes
- ❑ No
- ❑ We are already participants in the CBPRs program

ASK K5 IF YES IN K4

K5. When do you expect your CBPR application to be approved?

- ❑ Our CBPR application is already approved
- ❑ Within a year
- ❑ Within 1-3 years
- ❑ More than three years
- ❑ We do not intend to use CBPR
- ❑ Do not know

K6a. Are you using governance, risk management and compliance (GRC) software as part of your privacy management program?

- ❑ Yes
- ❑ No
- ❑ Don't know

ASK K6B IF YES IN K6A

K6b. Is your use of GRC software for privacy purposes limited to the privacy team specifically, or do other employees outside of the privacy team use it as well? ***Please select the response that best applies***

- ❑ Only privacy team members use
- ❑ Privacy team members and employees with privacy responsibilities use
- ❑ Employees throughout the company use, with privacy responsibiliites and not

ASK K6C IF RESPONSE 2 IN K6B

K6c. Do the employees with privacy responsibilities outside of the privacy team also have security responsibilities?

- ❑ Yes
- ❑ No
- ❑ Don't know

Survey 2: IAPP Salary and Operations Survey 2017

A. Company Information

1. In this first section, we'll ask about the company you work for. Which sector listed below best describes how your company would be classified?
   - Aerospace and Defense
   - Banking
   - Business Services and Supplies
   - Capital Goods
   - Chemicals
   - Conglomerates (multiple sectors)
   - Construction
   - Consumer Durables
   - Diversified Financials
   - Drugs and Biotechnology
   - Education and Academia
   - Food, Drink or Tobacco
   - Food Markets
   - Government
   - Healthcare Equipment and Services
   - Hotels, Restaurants and Leisure
   - Household and Personal Products
   - Insurance
   - Materials
   - Media
   - Nonprofit
   - Oil and Gas Operations
   - Retailing
   - Semiconductors
   - Software and Services
   - Technology Hardware and Equipment
   - Telecommunication Services
   - Trading Companies
   - Transportation
   - Utilities
2. In what regions does your company have employees? Please select all that apply.
   - United States
   - Canada
   - Latin America (including Mexico)
   - United Kingdom
   - European Union, not including UK
   - Non-EU Europe
   - Africa
   - Middle East
   - Asia
   - Australia
   - New Zealand

3. In what region are you currently based? Select one response only.
   - United States
   - Canada
   - Latin America (including Mexico)
   - United Kingdom
   - European Union, not including UK
   - Non-EU Europe
   - Africa
   - Middle East
   - Asia
   - Australia
   - New Zealand
4. What is the primary location of your company's headquarters? Select one response only.
   - United States
   - Canada
   - Latin America (including Mexico)
   - United Kingdom
   - European Union, not including UK
   - Non-EU Europe
   - Africa
   - Middle East
   - Asia
   - Australia
   - New Zealand

IF A4=U.S., Latin America, Middle East, Africa, Asia

5. Keeping in mind this survey is confidential and your individual information will not be shared, please tell us (as accurately as you can) your company's annual revenue in US dollars.
   Your best estimate is fine. $_____

IF A4=Canada

Keeping in mind this survey is confidential and your individual information will not be shared, please tell us (as accurately as you can) your company's annual revenue in Canadian dollars.
Your best estimate is fine. $_____

IF A4=UK

Keeping in mind this survey is confidential and your individual information will not be shared, please tell us (as accurately as you can) your company's annual revenue in British Pounds?
Your best estimate is fine. £_____

IF A4=EU or Non-EU Europe

Keeping in mind this survey is confidential and your individual information will not be shared, please tell us (as accurately as you can) your company's annual revenue in euros?
Your best estimate is fine. €_____

IF A4=Australia

Keeping in mind this survey is confidential and your individual information will not be shared, please tell us (as accurately as you can) your company's annual revenue in Australian dollars?
Your best estimate is fine. $_____

IF A4= New Zealand

Keeping in mind this survey is confidential and your individual information will not be shared, please tell us (as accurately as you can) your company's annual revenue in New Zealand dollars?
Your best estimate is fine. $_____

6. What is the total number of employees in your company (full-time and part-time)? We're looking for the total number for your entire company. If you work in a subsidiary of another corporation, please answer for the subsidiary only.

   Enter your best estimate below, then choose the category it falls into

_____

- 1-250
- 250-1,000
- 1,000-5,000
- 5,001-25,000
- 25,001+

ASK A7 IF HQ IS IN US IN A4

7. In what state is your company headquarters located? Select one response only.
   - Alabama
   - Alaska
   - Arizona
   - Arkansas
   - California
   - Colorado
   - Connecticut
   - Delaware
   - Florida
   - Georgia
   - Hawaii
   - Idaho
   - Illinois
   - Indiana
   - Iowa
   - Kansas

- Kentucky
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Tennessee
- Texas
- Utah
- Vermont
- Virginia
- Washington
- Washington, D.C
- West Virginia
- Wisconsin
- Wyoming

ASK A8 IF HQ IS IN EU IN A4

8. In what country is your company headquarters located? Select one response only.
    - Austria
    - Belgium
    - Bulgaria
    - Croatia
    - Cyprus
    - Czech Republic
    - Denmark
    - Estonia
    - Finland

- France
- Germany
- Greece
- Hungary
- Ireland, Republic of
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- United Kingdom

ASK A8A OF ALL

A8A. Which of the following best describes where your company's headquarters is located? Select one response only.

- Large urban area (population more than 1,000,000)
- Small urban area (population between 200,000 and 1,000,000)
- Town or suburban area (population between 2,500 and 200,000)
- Rural area (population less than 2,500)

B. Salary information

One of the main goals of this study is to determine how compensation for privacy professionals is changing over time. The following questions will ask about your own compensation. Again, remember that your responses will be kept completely confidential and will be analyzed in aggregate only, grouped with all responses from the survey.

IF A3=U.S., Latin America, Middle East, Africa, Asia

1a. What is your current base salary expressed in U.S. dollars? $_____

IF A3=Canada

1b. What is your current base salary expressed in Canadian dollars? $_____

IF A3=UK

1c. What is your current base salary expressed in British Pounds? £_____

IF A3=EU or Non-EU Europe

1d. What is your current base salary expressed in euros? €_____

IF A3=Australia

1e. What is your current base salary expressed in Australian dollars?
$_____

IF A3= New Zealand

1f. What is your current base salary expressed in New Zealand dollars?
$_____

ASK ALL

2. Did you receive a raise in your base salary during the past 12 months?
- Yes
- No

IF B2=YES

3. Regarding your last raise, by what percent did it raise your base annual salary? _____%

4. Did you receive any bonus payments related to your privacy role above your base salary during the past 12 months?
- Yes
- No

ASK B5a-B6 IF YES TO BONUS IN B4.

IF A3=U.S., Latin America, Middle East, Africa, Asia

5a. How much of a bonus have you received in the past 12 months, expressed in U.S. dollars?
$_____

IF A3=Canada

5b. How much of a bonus have you received in the past 12 months, expressed in Canadian dollars?
$_____

IF A3=UK

5c. How much of a bonus have you received in the past 12 months, expressed in British Pounds?
£_____

IF A3=EU or Non-EU Europe

5d. How much of a bonus have you received in the past 12 months, expressed in euros?
€_____

IF A3=Australia

5e. How much of a bonus have you received in the past 12 months, expressed in Australian dollars?

$_____

IF A3= New Zealand

5f. How much of a bonus have you received in the past 12 months, expressed in New Zealand dollars?

$_____

6. Which of the following best describes your bonus structure? Select one response only.

- The amount I receive in bonus payments depends on the overall performance of the company or other factors, not on the performance of my privacy program.
- The amount I receive in bonus payments depends on a combination of the company's overall performance and on my individual performance objectives.
- The amount I receive in bonus payments depends exclusively on my own performance objectives, indirectly related to the performance of the company's privacy program.
- The amount I receive in bonus payments directly depends on the performance of my company's privacy program as measured by factors such as program maturity, resolution of audit gaps, reduction of privacy incidents or other performance indicators.
- I do not know what my bonus depends on.

C. Next, we have some questions about your background.

1. Are you the company's Privacy Leader, or is that someone else?

- Yes, I am the Privacy Leader
- Someone else is the Privacy Leader

2. Which certifications do you hold? Please check all that apply.

- CIPP/US (CIPP)
- CIPP/E
- CIPP/G
- CIPP/C
- CIPT
- CIPM
- CISSP
- CISM
- CISA
- CRM
- CBCP
- Certified Public Accountant (CPA)
- Other _____
- None

3. Which of the following levels best describes your position in your company? Note, these are organized in descending order of seniority. Please select the one response that is closest to your position.

- C-Suite level
- Executive Vice President level
- Senior Vice President level
- Vice President level
- Director level (not Board)
- Lead Counsel level
- Assistant or Associate Counsel level
- Manager level
- Supervisor
- Solutions Architect
- Coordinator
- Individual Contributor
- Analyst
- Other (specify)

4. What is your specific title?

_____

5. Are you a designated “Data Protection Officer”?

- Yes
- No
- I don’t know

6. How many years have you been in your current position?

_____

7. What are your total years of privacy experience?

_____

8. Was privacy your first professional job?

- Yes
- No

ASK C9 IF NO IN C8

9. What type of position did you hold immediately before beginning your privacy career? Select one response only

- Corporate Ethics
- Finance and Accounting
- Government Affairs
- Product Manager
- Product Engineer
- Product Designer
- Human Resources

- Information Security
- Information Technology
- Internal Audit
- Legal
- Marketing
- Mergers and Acquisitions
- Physical Security
- Procurement
- Public Relations
- Records Management
- Regulatory Compliance
- Sales
- Supply Chain and Logistics
- Other (PLEASE SPECIFY)

ASK ALL

10. What was the last level of education that you completed?

- High school/secondary education
- Vocational or technical school
- Some college, no degree
- Associates degree or other two year course
- College /undergraduate (4 year)
- Master's degree (MA, MS, MLS, etc.)
- Doctoral degree (PhD)
- Professional/Postgraduate degree (MBA, MD, JD, etc.)
- Other

Survey 3: Preparing for the GDPR: DPOs, PIAs, and Data Mapping 2016

1. Does the organisation you work for have customers and/ or employees in the European Union?
   - Yes
   - No
   - Don't know
2. Does your organisation fall under the scope of the General Data Protection Regulation?
   - Yes
   - No
   - Don't know
3. Which of the following best describes your organisation's preparation for the GDPR?
   - What is the GDPR?
   - We have a preliminary plan
   - We have a plan and have begun implementation
   - We have a plan and are well into implementing it
   - We are fully compliant already
   - Don't know
4. With regard to the GDPR's requirement that certain organisations appoint a Data Protection Officer (DPO), which of the following best describes your organisation?
   - This requirement does not apply to us
   - We already have a DPO
   - We do not have a DPO but we will be appointing someone internally to fill the role
   - We intend to hire a new employee to serve as our DPO
   - We intend to outsource the DPO role
   - One of our affiliates has a DPO that we will share
   - Don't know

Those with DPO in place

5. With regard to the DPO position, which of the following is true?
   - Our privacy leader is our DPO
   - Someone in our privacy department (other than the privacy leader) is our DPO
   - We have trained someone who was not already filling a privacy function to serve as our DPO
   - We have more than one person serving in a DPO role
   - We have a DPO in each EU member state where we have an office or collect personal data
   - Don't know
6. Your organisation's DPO reports to
   - The Chief Privacy Officer/ Privacy leader
   - A position higher up the corporate ladder from the CPO/ privacy leader
   - A position on the same organisational level with the CPO/ privacy leader
   - A position lower on the organisational ladder from the Chief Privacy Officer/ privacy leader

Those who intend to appoint a DPO

7. With regard to the DPO position, which of the following is true?

- The Chief Privacy Officer/privacy leader will be the DPO
- Someone in our privacy department (other than the privacy leader) will be the DPO
- We will train someone who was not already serving a privacy function to be the DPO
- We will have more than one person serving in the DPO role
- We have a DPO in each EU member state where we have an office or collect personal data
- Don't know

8. Your organisation's DPO will likely report to
   - The Chief Privacy Officer/ Privacy leader
   - A position higher up the corporate ladder from the CPO/ privacy leader
   - A position on the same organisational level with the CPO/ privacy leader
   - A position lower on the organisational ladder from the Chief Privacy Officer/ privacy leader
9. Which of the following are barriers to completing privacy assessments (select all that apply)?
   - We don't have enough time/bandwidth
   - We lack internal support from leadership or other departments
   - We lack the right tools
   - We don't have the budget
   - We have the training or knowledge
   - We don't see the need or value
   - Other (please elaborate)
10. Which of the following, if any, describe your organisation's motivations for conducting privacy assessments (select all that apply)?
    - Compliance with the organisation's own information governance policy
    - Compliance with the EU's GDPR
    - To meet internal information security/ audit requirements
    - As part of vendor risk management
    - Compliance with U.S federal or state laws
    - For data breach preparedness
    - Our business partners request them
11. What tools do you use to conduct or record the results of your privacy assessments (select all that apply)?
    - We do it manually/informally with email, spreadsheets, and in-person communication
    - We use a system developed internally
    - We use governance, risk management and compliance (GRC)
    - We outsource our assessments to external consultants/ law firms
    - We use a commercial software tool designed specifically for privacy assessments
    - Don't know
12. Approximately how many privacy assessment (including DPIAs, PIAs, etc.) does your organisation conduct annually?
    - 1-2
    - 3-10
    - 11-50

- 51-100
- 101-500
- 501-1,000
- 1,000+
- Don’t know

13. How long does it typically take your privacy assessment to be completed?
    - <1 business day
    - 1-5 business days
    - 6-10 business days
    - More than 2 weeks
    - Up to one month
    - More than one month
    - Don’t know
14. Which of the following departments are involved or consulted in your organisation’s privacy assessments (select all that apply)?
    - Privacy
    - Information Security/ Cybersecurity
    - Legal
    - IT
    - Compliance
    - DPO
    - Product development/ engineering
    - Human resources
    - Marketing
    - External law firm
    - C-suite/ management
    - Regulators
    - R&D
15. How long do you maintain records of privacy assessments?
    - Indefinitely
    - >5 years
    - 3-5 years
    - 1-2 years
    - <one year
    - Don’t know
16. Which of the following are barriers to completing a data inventory mapping project for privacy purposes (select all that apply)?
    - Lack of internal resources/ staff
    - It’s a low priority for the organisation
    - Too busy, focussed on other projects
    - These projects are done by others (e.g. IT/ security)
    - Lack budget for external consultants or suppliers
    - It cannot be maintained so no reason to start
    - Don’t know
17. What tools do you use to perform data inventory and mapping (select all that apply)?
    - We do it manually/informally with email, spreadsheets, and in-person communication

- We use a system developed internally
- We use governance, risk management and compliance (GRC)
- We outsource our assessments to external consultants/ law firms
- We use a commercial software tool designed specifically for privacy assessments
- Don’t know

18. Which of the following departments are involved or consulted in data inventory and mapping projects (select all that apply)?
    - Privacy
    - Information Security/ Cybersecurity
    - Legal
    - IT
    - Compliance
    - DPO
    - Product development/ engineering
    - Human resources
    - Marketing
    - External law firm
    - C-suite/ management
    - Regulators
    - R&D
19. How do you maintain your data inventory/mapping projects?
    - Reviewed regularly by the privacy team
    - Reviewed on an ad hoc basis
    - We use external consultants to keep up to date
    - It’s not been updated since first produced
    - We use an automated tool to maintain the dat inventory
    - Don’t know
20. How are your data mapping/inventory projects usually funded?
    - From the privacy budget
    - From the IT, security, or compliance budget
    - It’s jointly funded by privacy and the IT, security, or compliance budgets
    - Don’t know
    - Other (please describe)

Survey 4: Getting to GDPR compliance: risk evaluation and strategies for mitigation

1. Does your organisation fall under the GDPR?
    - Yes
    - No
2. How risky is non-compliance with the following GDPR obligations (scale of 1-5, with 1 being no risk and 5 being high risk)
    - Preparation for breach
    - Data inventory/mapping
    - Obtaining consent
    - International data transfers
    - Maintain record keeping
    - Conducting DPIAs
    - Operationalising right to be forgotten
    - Data subjects request
    - Establish legit interest
    - Data portability
    - Appoint DPO
3. How will organisations mitigate risk for
    - Breach notification
    - Data inventory/ mapping
    - Obtaining consent
    - International data transfers
    - Records of processing
    - DPIAs
    - Operationalising right to be forgotten
    - Data subjects requests
    - Legitimate interests
    - Data portability
    - Appointing DPO

    Training – technology – status quo – staff – outside legal – outside consulting
4. What are the biggest barriers to GDPR compliance
    - Complexity of law
    - Inadequate budget
    - Too little time
    - Lack of qualified staff
    - Shortage of tech tools
5. When does your organisation expect to be GDPR compliant by
    - By end of 2017
    - By end of March 2018
    - By May 25, 2018
    - After May 25, 2018
    - Not sure

Survey Findings on Use of and Views about Payment through Mobile Phones in Hong Kong

1. Do you use cash or non-cash for daily expenses?
    - Be accustomed to using more cash
    - Be accustomed to using more cash
    - Both are similar
    - Cash only or cash only
    - Don't know/hard to say
2. How often do you use mobile wallet to pay or spend?
    - Often
    - In the middle
    - Rarely
    - Absolutely not
    - No smart phone
3. How often do you use mobile wallet to pay or spend?
    - Often
    - Between
    - Very few
    - No
    - No use of smartphone
4. Do you think that the government should launch policies to encourage people to use mobile wallets?
    - Should
    - Should not
    - Don't know/hard to tell
5. What are the main reasons why you use mobile wallets in Hong Kong?
    - No need to carry cash or credit cards
    - Exclusive discount or cash discount
    - Recommended by friends or family around you
    - Transfer or transfer money between friends or family easily
    - Completion of transaction time is short, no need to wait
    - Don't want to use cash/no money/no coins
    - Like to try new technology
    - You can track your own consumption records
    - Easy online shopping
    - Easy to use
    - Mobile phone stored value account can obtain interest return
    - Other
    - Don't know/hard to say
6. Overall, if Hong Kong uses a mobile wallet, are you satisfied with the smoothness and convenience of the entire transaction process?

- Very dissatisfied
- Not satisfied
- Ordinary
- Satisfaction
- Very satisfied
- Don't know/hard to say

7. Why didn't you use Hong Kong Mobile Wallet?
    - Personal Privacy Risk / No Confidence / Insecurity
    - Do not know how to use mobile wallet
    - Accustomed to using cash, credit cards or Octopus consumption
    - Stolen mobile wallet can cause property damage
    - Too few merchants accept mobile wallet transactions
    - Mobile wallet application trouble / no credit card
    - Mobile wallet transaction platform instability
    - Don't need / do not want to use
    - Mobile wallet is convenient for government monitoring
    - Not currently universal/untouched mobile wallet
    - Other
    - Don't know/hard to say
8. Would you like to call Hong Kong to try to use mobile wallet to pay or spend?
    - Willing
    - Unwilling
    - Half and a half
    - Don't know/hard to say
9. Some opinions suggest that “according to the family, Hong Kong people, people use their mobile wallet because the credit card or Octopus card is already very convenient.” How do you agree with this?
    - Less Hong Kong people use mobile wallet because Credit cards or Octopus are already very convenient.
    - Credit Card or Octopus Card Consumption Ratio Mobile wallet security.
    - Hong Kong as an advanced city, mobile wallet should be the universal use.
10. Some opinions suggest that "Compared to mobile wallets, it is safer to use a credit card or an Octopus card." How do you agree with this?
    - Less Hong Kong people use mobile wallet because Credit cards or Octopus are already very convenient.
    - Credit Card or Octopus Card Consumption Ratio Mobile wallet security.
    - Hong Kong as an advanced city, mobile wallet should be the universal use.
11. There are opinions that "Hong Kong as an advanced city should have universal use of mobile wallets. How do you agree with this?
    - Less Hong Kong people use mobile wallet because Credit cards or Octopus are already very convenient.
    - Credit Card or Octopus Card Consumption Ratio Mobile wallet security.
    - Hong Kong as an advanced city, mobile wallet should be the universal use.
12. Do you think the government should use the following policy to encourage the use of mobile wallets?
    - Improve the safety and reliability of mobile payment

- Providing service operators a fair competitive environment
- Promote the development of local financial technology industry
- Provide fee reductions for merchants that accept mobile wallet payments
- Provide mobile wallet payment channels for government fees
- Promote the fostering and exchange of talents in financial science and technology
- Other
- Don't know/hard to say

13. How often do you use mobile wallets to pay for or spend money outside Hong Kong?
    - Often
    - In the middle
    - Rarely
    - Absolutely not
    - No smart phone
14. Why do you use mobile wallets to pay or spend money? What are the differences between mainland China, other places, and fixed lines?
    - Inside China
    - Other places
    - Both have

Pew Research Center

Privacy and information sharing

1. A grocery store has offered you a free loyalty card that will save you money on your purchases. In exchange, the store will keep track of your shopping habits and sell this data to third parties. Would this scenario be acceptable to you, or not?
   - Yes
   - No
   - It depends
   - Refused
2. A new health information website is being used by your doctor's office to help manage patient records. Your participation would allow you to have access to your own health records and make scheduling appointments easier. If you choose to participate, you will be allowing your doctor's office to upload your health records to the website and the doctor promises it is a secure site. Would this scenario be acceptable to you, or not?
   - Yes
   - No
   - It depends
   - Refused
3. A new social media platform is being used by your former high school to help manage communications about a class reunion. You can find out the basic information about the reunion over email, but your participation on the social media site would reconnect you with old friends and allow you to communicate more easily with those who are attending. If you choose to participate, you will creating a profile using your real name and sharing a photo of yourself. Your access to the service is free, but your activity on the site would be used by the site to deliver advertisements it hopes will be appealing to you. Would this scenario be acceptable to you, or not?
   - Yes
   - No
   - It depends
   - Refused
4. Your insurance company if offering a discount to you if you agree to place a device in your car that allows monitoring of your driving speed and location. After the company collects data about your driving habits, it may offer you further discounts to reward you for safe driving. Would this scenario be acceptable to you or not?
   - Yes
   - No
   - It depends
   - Refused
5. Several co-workers of yours have recently had personal belongings stolen from your workplace, and the company is planning to install high-resolution security cameras that use facial recognition technology to help identify the thieves and make the workplace more secure. The footage would stay on file as long as the company wishes to retain it, and could be used to track various measures of employee attendance and performance. Would this scenario be acceptable to you or not?

- Yes
- No
- It depends
- Refused

6. A new technology company has created an inexpensive thermostat sensor for your house that would learn about your temperature zone and movements around the house and potentially save you on your energy bill. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room. Would this scenario be acceptable to you, or not?
   - Yes
   - No
   - It depends
   - Refused
7. In the course of making decisions about what personal information to share with various companies, at any point in the last month have you felt any of the following things?
   First at any point, have you felt
   - Discouraged with the amount of effort needed to understand what would be done with your data
   - Confused by the information provided in a privacy policy
   - Confident that you understood what would be done with your data
   - Impatient because you wanted to learn more but needed to make a decision right away
     Yes – No – Refused