PCPD
HK
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

2018 Study Report on Implementation of Privacy Management Programme by Data Users

5 March 2019

Table of Contents

I. Executive Summary

The Privacy Commissioner for Personal Data, Hong Kong (**PCPD**) participated in the Privacy Sweep (**Sweep**) of the Global Privacy Enforcement Network (GPEN) for the sixth consecutive year in 2018.

2. The theme of the global Privacy Sweep 2018 is "Privacy Accountability". Eighteen privacy enforcement authorities (**PEAs**) from around the world, including the PCPD, participated in the Sweep. Participating PEAs are required to write out to organisations of their choice to assess the quality of the oragnisations' privacy practices in relation to a set of common indicators.

3. During the period between October and November 2018, the PCPD wrote to 44 organisations from different sectors inviting them to participate in the Sweep, of which 26 of them agreed to participate (**Participating Organisations**).

4. The PCPD's major observations from the Sweep are summarised below: -

- All Participating Organisations have internal data privacy policy (in compliance with legal requirements) and this has been embedded into everyday practices
- Although not a legal requirement under the Personal Data (Privacy) Ordinance (**PDPO**), majority of the Participating Organisations have appointed sufficiently senior level staff for handling privacy governance and management matters
- Majority of the Participating Organisations provide comprehensive training on personal data protection to their staff
- All Participating Organisations maintain privacy policies easily accessible on their websites
- Almost all Participating Organisations maintain a documented incident response procedure
- Only some of the Participating Organisations have a procedure in place to notify affected individuals and report the breach to the regulator

- Majority of the Participating Organisations conducted and documented Privacy Impact Assessment (**PIA**) before introducing a new product or service
- Some of the Participating Organisations maintained a comprehensive personal data inventory
- Some of the Participating Organisations maintained a record of data transfer to third parties

5. Accountability has become a key principle of data protection, and has been incorporated into many laws, regulations, and industry guidance. Ownership of the personal data held by data users belongs to data subjects, who entrust their personal data to data users for processing. Compliance with legal obligations aside, data users are ethically responsible for protecting such personal data as data custodians. Organisations in general that amass and derive benefits from personal data should ditch the mindset of conducting their operations to meet the minimum regulatory requirements only. They should instead be held to a higher ethical standard that meets the stakeholders' expectations. Data users are encouraged to handle personal data based on the three Data Stewardship Values: Respectful, Beneficial and Fair.

II. Objectives of the Sweep

6. GPEN was established in 2010 upon recommendation of the Organisation for Economic Co-operation and Development to foster cross-border co-operation among privacy regulators in an increasingly global market. The Sweep aims at: -

- Broadening public and business awareness of privacy rights and responsibilities
- Identifying privacy concerns which need to be addressed
- Encouraging compliance with privacy legislation

7. Since 2014, the PCPD has advocated organisations develop their own Privacy Management Programme (**PMP**) which manifests the accountability principle. Organisations should embrace personal data protection as part of their corporate governance responsibilities and apply them as a business imperative

throughout the organisation, starting from the boardroom. This can, not only build trust with clients, but also enhance their reputation as well as competitiveness. The adoption of the accountability approach in handling personal data through implementation of PMP becomes a global trend for orgnaisations. The European Union's General Data Protection Regulation (**GDPR**), which came into force on 25 May 2018, now incorporates the accountability principle and data controllers are accountable for and required to demonstrate compliance with the data processing principles: article 5(2) of the GDPR.

8. The Sweep 2018 aimed to assess how well organisations have implemented accountability principle through PMP and their ability to manage privacy risk in all business processes. The PCPD would also like to understand the practical difficulties encountered by organisations in the course of implementing PMP to facilitate us providing assistance to organisations for implementing PMP.

9. The PCPD approached 44 organisations from different sectors (i.e. insurance, financial, telecommunications, public utilities and transportation) inviting them to participate in the Sweep. These organisations were selected based on their size and the vast amount of personal data held by them. The PCPD received response/partial response from 26 Participating Organisations.

III. Methodology of the Sweep

10. The PCPD conducted the Sweep by: -

- Visiting the websites of the Participating Organisations and locating their privacy policy
- Seeking organisations' response in respect of a set of the pre-defined questions (see paragraph 11 below)

11. All participating PEAs used the pre-defined questions set by the GPEN supplemented by their own questions to conduct the assessment. The pre-defined questions set by the GPEN are:

- The organisation has an internal data privacy policy (consistent with legal requirements), and it has been demonstrated that this has been embedded into everyday practices
- The organisation has someone at a sufficiently senior level responsible for privacy governance and management
- The organisation ensures staff are given training regarding the protection of personal information by informing them of organisational privacy policies, procedures and best practices
- The organisation monitors their performance in relation to data protection standards (i.e. by conducting self-assessments and/or audits of their privacy programme and in relation to complaints/enquiries/breaches)
- The organisation actively maintains policies to explain how they handle personal data, and are these easily accessible to customers and the general public
- The organisation maintains a documented incident response procedure
- In the event of a breach, the organisation has a procedure in place to notify affected individuals and report the breach to the regulator
- The organisation maintains an incident log detailing all breaches that occur
- The organisation has policies and procedures in place to respond to requests and complaints from individuals, and other external enquiries (such as the regulator)
- The organisation has documented processes in place to assess the risks associated with new products, services, technologies and business models (for instance, the organisation can demonstrate that they conduct privacy impact assessments)
- The organisation maintains an inventory of the personal data held by them
- The organisation maintains a record of data flows (i.e. data shared with third parties)

12. PEAs would need to assess the responses based on the pre-defined questions above. The responses to each question should be given a rating: "Very Good", "Satisfactory", "Poor" or "Failed to Specify".

13. The original questionnaire and rating criteria pre-defined by the GPEN for this Sweep purpose are at **Appendix A** and **Appendix B**.

14. As some of these indicators required subjective judgment of the examining officers concerned, the responses from the Participating Organisations were examined by five officers in the PCPD to ensure the objectiveness of the assessment. Prior to the review and analysing of the responses from the Participating Organisations, the five officers discussed with a view to achieving a consistent rating standard.

15. Additional questions have also been raised by the PCPD with the organisations for the purpose of facilitating us to provide assistance to organisations for implementing PMP. The questions are listed below: -

- What are the practical difficulties that the organisation encountered when implementing accountability?
- Can the organisation share with us their good strategies and practices in personal data protection?
- What kind of assistance/support that the organisation expects from the PCPD for implementing accountability in your organisation?

IV. The Global Sweep Results

16. Eighteen PEAs around the world, including the PCPD, made contact with a total of 356 organisations from various sectors including (but not limited to) education, electronic commerce, finance and insurance, health industry, legal, marketing, public sector (including central and local government), retail, telecommunications, tourism, transport and leisure. Major observations from the global Privacy Sweep are listed below.

- Nearly three quarters of organisations across all sectors and jurisdictions had appointed an individual or team who would assume responsibility for ensuring that their organisation complied with relevant data protection rules and regulations

- Organisations were generally found to be quite good at giving data protection training to staff, but often failed to provide refresher training to existing staff
- When it comes to monitoring internal performance in relation to data protection standards, many organisations were found to fall short, with around a quarter who responded having no programmes in place to conduct self-assessments and/or internal audits
- The organisations that indicated that they have monitoring programmes in place generally gave examples of good practice, noting that they conduct annual audits or reviews and/or regular self-assessments
- Over half of the organisations surveyed indicated that they have documented incident response procedures, and that they maintain up to date records of all data security incidents and breaches. However, a number of organisations indicated that they have no processes in place to respond appropriately in the event of a data security incident

V. The PCPD's Sweep Results

17. The handling of personal data and data protection policies and measures of organisations may change over time. Hence, the PCPD's Sweep results only represent the position surveyed as of October to November 2018.

18. Moreover, the Sweep was a coordinated research exercise and was not a compliance check or formal investigation. Therefore it is not appropriate for the PCPD to disclose the specific results and findings for each Participating Organisation. The results and findings set out below are aggregated results based on the responses from the Participating Organisations.

19. The PCPD's observations are largely in line with the global Sweep results as discussed above. Major observations by the PCPD during the Sweep are summarised under the following headings: -

- Policies, procedures and governance
- Monitoring, training and awareness

- Transparency
- Responsiveness and incident management
- Risk assessment, documentation and data flows

Policies, procedures and governance

20. All Participating Organisations (100%) indicated that they have internal data privacy policy (in compliance with legal requirements) and this has been embedded into everyday practices.

21. Although it is not a legal requirement under the PDPO, majority of the Participating Organisations (19, 73.08%) have appointed a sufficiently senior level staff for handling privacy governance and management matters. Some of them have a committee comprising of representatives from different divisions responsible for privacy governance and management. Five Participating Organisations (19.23%) stated that they had assigned someone but not at a senior level to handle privacy governance and management matters. The rest of the Participating Organisations (7.69%) did not specify the level of the persons responsible for privacy governance and management matters.

22. The responses above are encouraging, showing that organisations recognise that personal data protection is an integral part of their business and have invested resources and have dedicated personnel to handle personal data protection.

Monitoring, training and awareness

23. All Participating Organisations (100%) stated that they understood the importance of providing staff with training on personal data protection. 17 Participating Organisations (65.38%) provide comprehensive training on personal data protection to their staff, including induction training for newcomers, regular refresher training for current employees and attendance at training workshops provided by the PCPD. One of the organisations requires their staff to take a PDPO training course and pass the test regularly. The training provided by the other eight Participating Organisations (30.77%) was not comprehensive (e.g. the refresher training was not conducted on a regular basis).

24. One Participating Organisation (3.85%) only asked their staff members to read and acknowledge their understanding of the organisation's privacy policy. The PCPD considered that such practice was unsatisfactory.

25. As for the self-assessment or audit on data protection standards, half of the Participating Organisations (13, 50%) conducted audit on statutory compliance on a regular basis and some of them engage external auditor to conduct their audit. However, eleven Participating Organisations (42.31%) admitted that the self-assessment or audit would not be conducted regularly. The rest of two Participating Organisations (7.69%) did not specify whether self-assessment or audit on data protection standards was conducted.

Transparency

26. All Participating Organisations (100%) maintain privacy policies which are easily accessible on their websites. An area that can be improved is that the privacy policy of one Participating Organisation is available in Chinese only.

27. 23 Participating Organisations (88.46%) indicated in their privacy policies that they have appointed a data protection officer and provided the contact details (e.g. address and email address). However, the rest of the three Participating Organisations (11.54%) did not specify whether they had a dedicated data protection officer. Among these three Participating Organisations: -

- one stated that customers may contact the organisation's Manager for privacy-related matters
- the remaining two stated that customers may contact Customer Service Department for access or correction of personal data

Responsiveness and incident management

28. A number of large scale data leakage incidents came to light in Hong Kong in 2018 and have heightened public awareness and concern regarding the protection of personal data by data users. A set of comprehensive mechanisms and procedures

in place to respond to data breach incidents can facilitate organisations handle such incidents effectively, and to mitigate the damage that may be caused to the impacted data subjects and to such organisations' reputation.

29. One Participating Organisation (3.85%) did not specify whether it had maintained a documented data breach incident response procedure. The rest of the 25 Participating Organisations (96.15%) expressed that written data breach incident response procedure is in place, modelled on the requirements in the "*Guidance on Data Breach Handling and the Giving of Breach Notifications*" issued by the PCPD. The findings revealed that organisations understand the gravity of the consequence of a data breach incident.

30. Regarding the procedure in place to notify impacted individuals and the regulator if necessary, the situation is less satisfactory: -

- Only 16 Participating Organisations (61.54%) have devised such procedure
- Four Participating Organisations (15.38%) do not have such procedure in place, and they would only decide what and how to do after a data breach incident has occurred
- Six Participating Organisations (23.08%) did not specify if such procedure is in place

31. 24 Participating Organisations (92.31%) maintain an incident log detailing all breaches that occur. The remaining two (7.69%) did not specify on this aspect.

32. As for whether the organisation has policies and procedures in place to respond to requests and complaints from individuals, and external enquiries (such as the regulator), 24 Participating Organisations (92.31%) have devised relevant policies and procedures and some of these organisations have a special team responsible for these matters. One Participating Organisation (3.85%) stated that while it had established a procedure to handle general enquires from customers, no policy or procedure is in place to respond to external enquiries made or complaint cases referred by regulatory bodies. One Participating Organisation did not specify on this aspect.

Risk assessment, documentation and data flows

33. It is not a responsible personal data protection approach by taking reactive remedial actions only after an incident has occurred. Conducting PIA before launching a new project, product or service can help organisations identify and assess the potential privacy risks upfront in an early stage and to make necessary improvements.

34. 23 Participating Organisations (88.46%) conduct a PIA before introducing new products, services, technologies and business models so as to understand the potential privacy risks. Two Participating Organisations (7.69%) stated that they conduct PIA but no written record is kept. The remaining Participating Organisation (3.85%) did not specify on this aspect. The above result reflected that organisations recognised the importance of "prevention".

35. Only seven Participating Organisations (26.92%) maintain a comprehensive personal data inventory recording categories of personal data they held, location for storage, retention period, use and security measures adopted. The personal data inventories maintained by most of the Participating Organisations (14, 53.85%) are incomprehensive, as such inventories cover customers' personal data but not employees' personal data. Four Participating Organisations (15.38%) responded that they had only maintained personal data inventory for certain departments or projects and one Participating Organisation (3.85%) admitted that it did not maintain any personal data inventory. The remaining Participating Organisation did not specify whether any personal data inventory is maintained. The above revealed that organisations do not have a comprehensive picture of the personal data in their possession.

36. Organisations may transfer personal data to third parties due to business needs. Recording the personal data flow would certainly help organisation to understand the source of personal data and details of the data transfer so as to facilitate future checking by the organisations. The performance of the Participating Organisations in this area was not satisfactory. Only seven Participating Organisations (26.92%) maintain a comprehensive record of data flows. The

records of data flows maintained by other seven Participating Organisations were not in details. Six Participating Organisations (23.08%) did not maintain such records. The remaining six Participating Organisations did not specify whether they maintained such record.

37. The Sweep Statistics is at **Appendix C**.

38. With regard to the additional questions raised by the PCPD (see paragraph 15 above), the responses from Participating Organisations are summarised as below: -

Practical difficulties encountered when implementing accountability

39. Half of the Participating Organisations considered the "Privacy Management Programme: A Best Practice Guide" issued by the PCPD can effectively assist them in constructing their own programme, and they did not encounter significant difficulties during the implementation process.

40. The remaining Participating Organisations highlighted some difficulties which are summarised below: -

- Lack of adequate resources, including finance, expertise and tools
- Difficulty to enhance the awareness of personal data protection to the employees whose duties do not involve personal data handling
- Some employees disregard the importance of personal data protection as compared to other regulatory requirements (e.g. anti-money laundering and anti-corruptions) as serious penalty are imposed for violation of those requirements
- Difficulty to adopt a common approach in handling personal data within an organisation as different departments have their own need and practices. In addition, it is not practicable to record the personal data processing in large-scale organisations
- The number of complex data processing systems in use within large organisations makes it difficult to have a comprehensive personal data inventory

Good strategies and practices in personal data protection

41. Some Participating Organisations shared with us their good strategies and practices in personal data protection:-

Privacy Policy

- Establishes a clear data governance framework which sets out the roles and responsibilities of various departments. In addition, Data protection manuals and guidelines are made available on the organisation's intranet to enable the staff to keep abreast of the latest regulations and development
- Adopts minimal data collection policy
- Secures support from the top executives that personal data protection is one of the most critical tasks of the organisation

Training and Education

- Invites in-house lawyers to explain the PDPO to employees in order to enhance staff's awareness of use of personal data
- Organises interactive training to strengthen the culture of personal data protection
- Tests whether employees can apply relevant knowledge in their daily work after training
- Employs appropriately skilled persons with the necessary skills and knowledge in personal data protection

Data Breach Handling

- Develops an online platform for incident reporting so that employees can have an efficient and easy way to report any potential data privacy incidents; and such incidents can be properly tracked and monitored

Communication

- Nominates staff of different levels as "Data Protection Focal Point"
- Holds quarterly meetings to address privacy concerns and manages controls of operations

- Forms a working group with representatives from different departments and led by the Data Protection Officer. Regular meeting were held to discuss privacy related issues and best practices were shared. Findings from monitoring were escalated and reported to the management level committees, including the progress of the remediation actions

Ongoing Assessment and Revision

- Conducts annual data audit to find out potential non-compliance with the PDPO. Non-compliance issues, depending on the risk and implications, are escalated to the appropriate level of senior management
- Reviews the questions in PIA to ensure all privacy risks can be identified in the planning stage of the business initiatives. PIA is required to be submitted to a dedicated committee for review and approval

Assistance or support expected to be provided by the PCPD in implementing PMP

42. Participating Organisations would like the PCPD to provide the following assistance or support to facilitate their implementation of PMP: -

- To provide more training seminars, including tailor-made workshops for different sectors and regular cases sharing sessions
- To provide more sample documents for organisations to use for each process in order to achieve the accountability principle
- To provide seminars targeted at senior management
- To regularly share common mistakes in handling personal data through newsletter
- To issue guidelines and best practices on personal data handling for organisations as references
- To certify and publicise organisations' good practices in personal data protection

43. The PCPD will consider the above recommendations. In fact, to keep organisations abreast of the latest practice in handling personal data, the PCPD has from time to time issued or revised a wide range of useful guidance on compliance

with the PDPO. The PCPD has a Data Protection Officers' Club which issues monthly newsletter that provides updates on the PCPD and the privacy news. In future, the PCPD will continue to organise seminars and professional workshops on PMP to help organisations prepare their own PMP manual and construct a comprehensive programme.

VI. Conclusions and Recommendations

44. Unlike the GDPR, the accountability principle and the related privacy management measures are not part of the PDPO requirements. The PCPD has advocated that organisations should develop their own PMP to demonstrate accountability. The appointment of data protection officers and the conduct of PIA are recommended good practices to achieve accountability.

45. The PCPD's Sweep Results revealed that comparing to those overseas countries which had explicitly stated the accountability principle in their laws, the performance of Hong Kong organisations in implementing voluntary PMP is satisfactory. It reflects that organisations give weight to personal data privacy protection, and are willing to commit more resources to this area. Nevertheless, the PCPD has the following recommendations to organisations in implementation of PMP: -

- **Provide adequate data protection training:** With increased pace and use of digitalisation in businesses, staff may access personal data of colleagues or customers in their daily work. Hence, organisations should ensure their staff understands the requirements under the PDPO and to observe the organisation's policy in relation personal data handling. In this connection, organisations should provide adequate and regular training by explaining the organisation's relevant policy and the requirements under the PDPO to newcomers and providing on-going training courses. If amendments are made to the organisation's policy in relation personal data handling or the PDPO, the organisation should notify its staff immediately

- **Conduct regular audit:** Conduct regular audit by dedicated persons/independent third party to ensure the policies and practices of the organisations are in compliance with the PDPO and to find out whether there is room for improvement

- **Handling of Data Breach Incident:** Devise written procedures in relation to the factors to be considered, mechanism and practice when assessing whether to give data breach notification to affected individuals and regulatory bodies. While organisations have invested resources in meeting the legal requirements to have privacy policy, as data breach notification is not a legal requirement, there was less focus on devising a procedure to deal with data breaches. The threat of cyber-attack is real and the risk of not having a data breach notification in place could be serious

- **Maintain a comprehensive personal data inventory:** The number of complex data processing systems in use within the organisation makes it even more important to maintain a personal data inventory. Each department of an organisation can prepare their own inventory which covers the personal data held by the respective department. The purpose of maintaining a comprehensive personal data inventory is to assist organisations to fully grasp the personal data they hold which would benefit the handling of personal data in the entire data life cycle

- **Maintain a record of data flow:** Recording the data flow can facilitate organisations to easily check and retrieve relevant information in future when necessary

46. It is a best practice for organisations to construct and implement a comprehensive PMP. Data stewardship should cover the overall business practices, operational processes, product and service design, physical architectures and network infrastructure. The PMP, supported by an effective ongoing review and monitoring process to facilitate its compliance with the requirements under the PDPO, serves as a strategic framework to assist organisations in building a robust

privacy infrastructure and to share mutual fairness, respect and benefit with their customers and employees.

Appendix A – The Sweep Questionnaire

Statement	Assessment			Evidence
	Achieved	Partially achieved	Not Achieved	*Please describe how each area has been achieved in practice, and provide evidence where possible.*
Your organisation has an internal data privacy (consistent with legal requirements) policy which has been embedded into everyday practices				
Your organisation has allocated someone at a sufficiently senior level to be responsible for privacy governance and management				
Your organisation ensures staff are given training regarding the protection of personal information, and you inform them of organisational privacy policies, procedures and best practices				
Your organisations performance is monitored in relation to data protection standards (i.e by				

conducting self-assessments and/or audits of your privacy programme and in relation to complaints / enquiries / breaches)				
Your organisation actively maintains policies to explain how you handle personal data, and these easily accessible to customers and the general public				
Your organisation maintains a documented incident response procedure				
In the event of a breach, your organisation has a procedure in place to notify affected individuals and report the breach to the regulator where necessary				
Your organisation maintains an incident log detailing all breaches that occur				
Your organisation has policies and procedures in place to respond to requests and complaints from				

individuals, and other external enquiries (such as the regulator)				
Your organisation has documented processes in place to assess the risks associated with new products, services, technologies and business models (for instance, you conduct privacy impact assessments)				
Your organisation maintains an inventory of your personal data holdings				
Your organisation maintains an inventory of any data flows (for example, data transfers to third parties)				

Appendix B – The Sweep Rating Criteria

RATING CRITERIA

The below criteria is for consideration when rating each organisation's response to PEA's queries. These examples are for guidance only, and PEAs may choose to adopt their own grading criteria.

Very Good

The organisation demonstrated that they have implemented the essential elements of accountability into everyday business practices and policies (as broken down into common indicators).

Examples of good practice may include:

- The organisation maintains a data privacy framework (consistent with legal requirements) which has become embedded into everyday practices.
- A data protection officer / privacy officer has been appointed, and/or there is someone at a sufficiently senior level responsible for privacy governance and management.
- Regular data protection training is given to staff (this would include training for new starters and refresher training for current employees).
- The organisation conducts regular self-audits, and regularly reviews its performance in relation to data protection standards.
- The organisation demonstrated that they maintain a clear privacy policy, which is easily accessible to customers and the general public.
- The organisation demonstrated that they have a documented incident response procedure, and has steps in place to notify affected individuals and the regulator.
- The organisation maintains an incident log which is regularly kept up to date.
- The organisation has policies and procedures in place to respond to requests and complaints from individuals, and other external enquiries (such as the regulator).
- The organisation has a documented processes in place to assess the risks associated with new products, services, technologies and business models (for instance, it conducts privacy impact assessments for all new projects).

- The organisation maintains an inventory of the personal data held by them and records data flows.

Satisfactory

The organisation showed some evidence of having implemented the essential elements of accountability (as broken down into common indicators), into business policies and practices, but they are lacking in some aspects and require improvement.

Examples may include:

- The organisation is either in the process of implementing a data privacy framework (consistent with legal requirements) or they have a partial framework which they aim to implement into everyday practices.
- A data protection officer / privacy officer has been appointed, but there is nobody at a sufficiently senior level responsible for privacy governance and management.
- Some data protection training is given to staff, but the organisation may fail to give refresher training, or only provides training for some employees.
- The organisation shows evidence of having conducted self-audits and reviews its performance in relation to data protection standards, but reviews should be more thorough and/or held more regularly.
- The organisation demonstrated that they have a privacy policy, but this may not be easily accessible to the general public, lacking key principles of data protection, or outdated.
- The organisation has some measures in place to deal with privacy-related concern and queries, and their ability to appropriately deal with a data breach was satisfactory, but may lack some essential steps and requires improvement.
- The organisation indicated that they records incidents, but may fail to keep this up to date, or fail to have set processes in place.
- The organisation shows some understanding of the importance of assessing risks associated with new products, services, technologies and business model, but may not have a written process and requires improvement.
- The organisation has some understanding of the sort of data they hold, but fails to maintain an adequate inventory of the personal data held by them and/or record data flows.

Poor

The organisation was not able to show any understanding of the practices which form the essential elements of accountability (as broken down into common indicators).

- The organisation demonstrates little to no understanding of privacy frameworks necessary in the everyday course of business.
- No data protection officer/privacy officer has been appointed.
- No data protection training is given to employees.
- The organisation does not monitor it performance by conducting reviews of its adherence to data protection standards.
- The organisation does not have a privacy policy.
- The organisation has no measures in place to deal with privacy related concerns or queries, and/or is unequipped to appropriately deal with a data breach.
- The organisation does not record or log incidents/breaches when they occur.
- The organisation demonstrates little to no understanding of the importance of assessing risks associated with new products, services, technologies and business model.
- The organisation has little to no understanding of the sort of data they hold, and fails to maintain an adequate inventory and/or record data flows.

Appendix C – The Sweep Statistics

The organisation has an internal data privacy policy (consistent with legal requirements), and it has been demonstrated that this has been embedded into everyday practices	**Number**	**Percentage**
Very good	19	73.08%
Satisfactory	7	26.92%
Poor	0	0%
Failed to specify	0	0%

The organisation has someone at a sufficiently senior level responsible for privacy governance and management	**Number**	**Percentage**
Very good	19	73.08%
Satisfactory	5	19.23%
Poor	0	0%
Failed to specify	2	7.69%

The organisation ensures staff are given training regarding the protection of personal information by informing them of organisational privacy policies, procedures and best practices	**Number**	**Percentage**
Very good	17	65.38%
Satisfactory	8	30.77%
Poor	1	3.85%
Failed to specify	0	0%

The organisation monitors their performance in relation to data protection standards (i.e by conducting self-assessments and/or audits of privacy programme and in relation to complaints / enquiries / breaches)	**Number**	**Percentage**
Very good	13	50.00%
Satisfactory	11	42.31%
Poor	2	7.69%
Failed to specify	0	0%

The organisation actively maintains policies to explain how they handle personal data, and are these easily accessible to customers and the general public	**Number**	**Percentage**
Very good	25	96.15%
Satisfactory	1	3.85%
Poor	0	0%
Failed to specify	0	0%

The organisation maintains a documented incident response procedure	**Number**	**Percentage**
Very good	24	92.31%
Satisfactory	1	3.85%
Poor	0	0%
Failed to specify	1	3.85%

In the event of a breach, the organisation has a procedure in place to notify affected individuals and report the breach to the regulator	**Number**	**Percentage**
Very good	12	46.15%
Satisfactory	4	15.38%
Poor	4	15.38%
Failed to specify	6	23.08%

The organisation maintains an incident log detailing all breaches that occur	**Number**	**Percentage**
Very good	23	88.46%
Satisfactory	1	3.85%
Poor	0	0%
Failed to specify	2	7.69%

The organisation has policies and procedures in place to respond to requests and complaints from individuals, and other external enquiries (such as the regulator)	**Number**	**Percentage**
Very good	19	73.08%
Satisfactory	5	19.23%
Poor	1	3.85%
Failed to specify	1	3.85%

The organisation has documented processes in place to assess the risks associated with new products, services, technologies and business models (for instance, the organisation can demonstrate that they conduct privacy impact assessments)	**Number**	**Percentage**
Very good	16	61.54%
Satisfactory	7	26.92%
Poor	2	7.69%
Failed to specify	1	3.85%

The organisation maintains an inventory of the personal data holdings	**Number**	**Percentage**
Very good	7	26.92%
Satisfactory	14	53.85%
Poor	4	15.38%
Failed to specify	1	3.85%

The organisation maintains a record of any data flows (i.e. data shared with third parties)	**Number**	**Percentage**
Very good	7	26.92%
Satisfactory	7	26.92%
Poor	6	23.08%
Failed to specify	6	23.08%