Twenty questions on privacy!

A Self-Check Basic Privacy and Security Compliance “Audit” Questionnaire

EY
Building a better working world

Introduction

Please have the person/persons responsible for (or most knowledgeable about) the privacy compliance and cyber security of the business print out and complete the Questionnaire by indicating their answer to each question by placing an "X" in the relevant space provided (but please complete only one printout and Questionnaire for the business). Please also include any comments or questions you may have for us in the "Comments" column.

If you are unsure or don't know you should answer "Don't Know". However, if you don't know for sure but suspect the answer is likely to be no you should answer "No". You should only answer "Yes" if you are certain the relevant practice is actually done by the business.

Once completed, please make a PDF copy of the completed Questionnaire and email it to your EY contact or direct to alec.christie@au.ey.com for scoring.

Once scored, one of our EY Law team will arrange a time to discuss the results (and briefly discuss any comments or questions you have noted in the "Comments" column) with the contact person listed below on a complimentary basis.

Key to results (spoiler alert!)

0-5 points:	The business is currently in great shape but you need to keep abreast of new developments. Sign up to receive our EY Law Privacy & Security Update.
6-10 points:	The business is in good shape but some areas need a little work. We are happy to assist the business get into great shape.
11-20 points:	The business needs to address certain shortcomings now! We are happy to discuss how the business may best address these shortcomings.
21 points and above:	"Run don't walk!", the business needs to significantly and urgently change many of its privacy and security practices. We are happy to assist you with this.

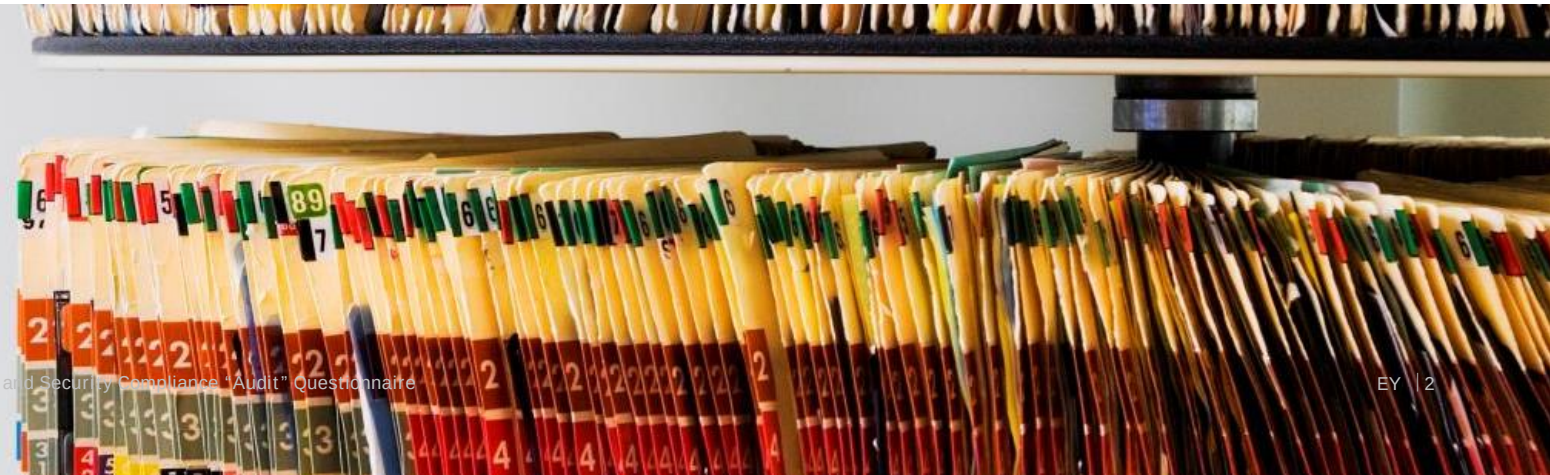
Who should we contact?

Please let us know who we should contact to discuss the results of this Questionnaire, once scored.

Contact Name:	
Company Name:	
Phone No:	
Email:	

Privacy policy

No.	Question	Yes	Don't know	No	Comments
1.	Does the business have a documented external/customer facing privacy policy?				
2.	Is the privacy policy on the website of the business (or otherwise publically available)?				
3.	Was the privacy policy updated to reflect the new APPs effective from 12 March 2014?				
4.	Is the privacy policy specific or tailored to the business and does it cover all of the current activities of the business?				

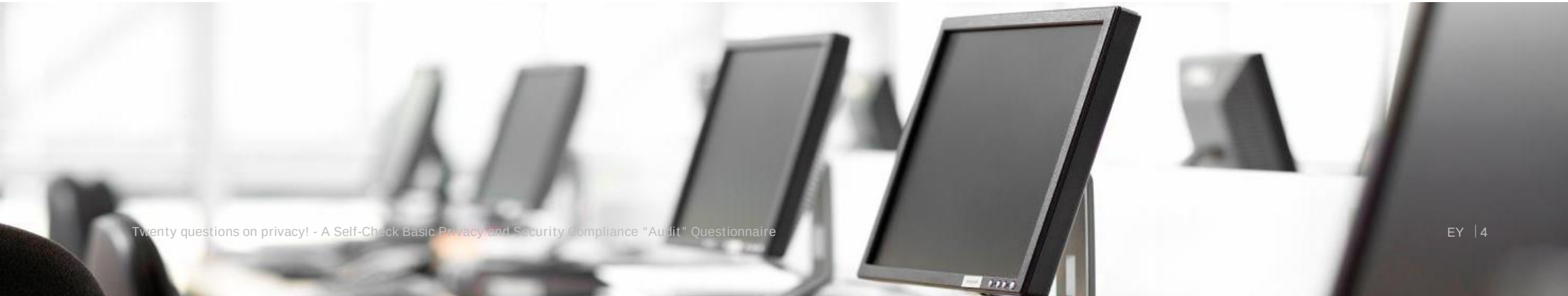


Collection process

No.	Question	Yes	Don't know	No	Comments
5.	Is the privacy policy always provided to individuals at or prior to the business collecting their personal information for the first time?				
6.	Does the business only collect personal information directly from the relevant individuals (i.e. not from third parties)?				
7.	Is all of the personal information collected by the business reasonably necessary for the current business activities of the business?				
8.	Do the purpose(s) notified for collection in the privacy policy fully cover: i. What the business actually uses the collected personal information for; and ii. Any planned future projects/uses of the personal information?				

Holding personal information

No.	Question	Yes	Don't know	No	Comments
9.	Do you know all of the types of personal information the business holds and where in the business and why such personal information is held?				
10.	Do you know (or can you easily identify): i. The notified purpose(s) for which all of the personal information held by the business has been collected (no matter when it was collected); and ii. Any contractual restrictions on its use?				
11.	Is it correct to say that none of the personal information held by the business has already been used for the notified purpose(s) for which it was collected?				
12.	If you answered "No" or "Don't Know" to Question 11, is it correct to say the business is required to retain that personal information by Australian law?				



Security of personal information

No.	Question	Yes	Don't Know	No	Comments
13.	Does the risk management framework of the business cover data breaches, cyber incidents, information and IT system security?				
14.	Does the business have (and implement) a document/data retention policy that includes the deletion or de-identification obligation of the business under the APPs?				
15.	Is the Board/senior management actively involved in, have oversight of and is responsible for the privacy compliance and cyber security of the business?				
16.	Does the business "audit" the security measures of all contractors (and other third parties) who have access to any of the premises, systems or personal information of the business?				

Disclosure of personal information

No.	Question	Yes	Don't know	No	Comments
17.	Do you know everyone the business discloses the personal information to/shares the personal information with?				
18.	Does the privacy policy list all of the types of persons to whom the business provides access to the personal information?				
19.	Does the privacy policy list all of the countries where the business provides access to the personal information?				
20.	For overseas disclosures, does the business require (i.e. contractually oblige) all recipients to comply with the APPs in respect of the personal information accessed by them?				

Next steps

Please take a PDF copy of your completed Questionnaire and email to your EY contact or directly to alec.christie@au.ey.com for scoring.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organisation and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organisation, please visit ey.com.

ED 0617

ey.com