

## Model GDPR Readiness Questionnaire

General Information	Response
Company name (legal and trading name)	
Account manager (for specific managing agents only)	
Questionnaire completed by? (include job title and contact details)	
Date form completed	
Role of Respondent Entity	

*Responses below should be in respect of any business handled on behalf of all Lloyd's Underwriters*

*Please provide a copy of any internal policy documentation related to the above questions.*

#	GDPR Awareness and Readiness	Response
1	Is your organisation aware of the changes to data protection law under GDPR and how it will impact your business?	
2a	Have you undertaken formal gap analysis against the requirements under GDPR?	
2b	Please describe any material gaps identified.	
3a	Have you initiated a project to achieve GDPR compliance?	
3b	Please describe the project (Include timescales, scope and whether you are happy to engage with Lloyd's / managing agents regarding alignment).	
4a	Do you expect to be compliant with GDPR by 25 May 2018?	
4b	What material challenges do you anticipate in achieving compliance?	

#	Staff Involvement and Awareness	Response
5	Does the project to comply with GDPR have the support of the board and executive?	
6a	Have you appointed / will you appoint a Data Protection Officer?	
6b	If you have answered 'No' to 6a, please advise who is responsible for data protection?	
6c	Please provide contact details.	
7	Do you have a training program in place to ensure all relevant staff are aware of GDPR requirements prior to 25 May 2018?	

#	Data Governance:	Response
8	Please specify the approximate volume of customer records processed by your organisation on behalf of Lloyd's Underwriters per annum?	
9	Have you created a record of your processing of personal data (also known as data mapping)?	
10a	Do you process special categories of personal data (known as sensitive personal data under the Data Protection Act), e.g. medical records, criminal records?	
10b	If you have answered 'Yes' to question 10a, and are processing data in respect of UK Insureds, do you have a written policy specifically for processing that data.	
11	Do you have any material outsource providers or subcontractors? If so, please confirm that they will be GDPR compliant by 25 May 2018.	

#	Fair Processing & Privacy Notices	Response
12	Do you intend to use the privacy notices based on the Model Core Information Notice? If not, please provide a copy of your privacy notice.	
13	Do you have a privacy notice on your website? If so, please provide a link.	

#	Data Subject Rights:	Response
14	Please confirm how many data subject access requests your organisation has received in the last 5 years?	
15a	Do you have policies and procedures in place to comply with a data subject's rights including their rights: to be informed; to access; to rectification; to erasure; to data portability; to object to direct marketing; and to object to automatic decision making.	
15b	Please provide additional information if you do not have policies and procedures in place to address these rights.	

#	Data Transmission and Data Residency:	Response
16a	Do you transfer personal data outside of the EU?	
16b	If so, what steps have you taken to ensure GDPR compliance?	
17	Do you have a documented process for storing data and retaining it in line with GDPR requirements?	
18	Has your organisation considered the GDPR Data Minimisation principle and reflected this in their relevant data retention policies?	
19a	Do you encrypt personal data when you transfer it to third parties?	
19b	Please describe how data that is transmitted is protected.	

#	Data Breach:	Response
20a	Have you documented your data breach notification procedures to meet GDPR requirements, and have all relevant staff been given adequate training in this?	
20b	Please provide additional information if 'No'.	
21a	Have you had any data breaches or large scale data losses in the last 12 months?	Please Select
21b	If so, please provide details including any regulatory response.	

Please set out any other steps you have planned to achieve GDPR compliance that are not identified in your answers to the questions above.	