Croner
HR · Tax · H&S · Reward

GDPR Questions & Answers		
No	Data Protection Compliance	Y/N
1	Will you be in a position to meet your obligations as a data controller or processor (as applicable) under the GDPR by 25 May 2018?	Yes
2	Do you have a DPO (Data Processing Officer)?	Yes
3	Do you have GDPR-compliant data protection and information security policies?	Yes
4	Can you confirm that you have appropriate measures in place to ensure that you, your staff and any subcontractors/sub-processors do not process personal data except on documented instructions from the client?	Yes
5	Do you have systems and procedures to notify recipients to whom personal data has been disclosed regarding data subject requests to rectify, erase or restrict the processing of their personal data?	Yes
6	Will you be providing training to your staff on compliance with the GDPR?	Yes
No	IT Security Policy	Y/N
7	Do you have a dedicated Information and Cyber Security team in the organisation?	Yes
8	Does an IT security policy exist and, if so, is it communicated to all employees?	Yes
9	Do you have policies and procedures in place for immediate reporting and investigation of suspected data security breaches, and remedial action in respect of actual breaches? Do you have a data security breach policy?	Yes
10	Is your organisation compliant and certified for any recognised IT Security and Data Protection standards such as ISO27001?	Yes
No	Physical Security	Y/N
11	Is the physical security of buildings providing Information Services to the company ensured?	Yes
12	Do you have specific precautions in place to ensure only authorised access to areas containing data processing, communications and storage equipment used for company data? This includes CCTV and Door Access Control.	Yes
13	Do you have a Disaster Recovery/Business Continuity plan? If so, When was the last test and what were the results? Has all necessary remediation been carried out and retested?	Yes

Croner
HR · Tax · H&S · Reward

No	Staff Security	Y/N
14	Do you have a dedicated team to support Information and Cyber Security?	Yes
15	Are staff Screened prior to employment?	Yes
16	Do Employment Terms & Conditions cover information security responsibilities including data protection?	Yes
17	Are staff adequately trained in IT Security and Data Protection principles?	Yes
18	Do you have internal process for reporting and managing security incidents?	Yes
19	Is staff access revoked immediately when leaving employment?	Yes
20	Do you have protection in place to ensure that staff credentials are not compromised by malware, remote access tools, keyboard loggers etc.	Yes
No	Data Security	Y/N
21	Are all Operating Systems in use fully supported and patched?	Yes
22	Is all software used to process company data is kept up to date?	Yes
23	Do vendor staff store company data on portable devices (inc. USB storage media)?	No
24	Are measures in place to prevent unauthorised access to Data from outside "hackers" (e.g. firewalls and other security measures) and is network monitoring in place?	Yes
25	Are restrictions in place to ensure control of data entering or leaving via internet access (via web browser, email, ftp, online storage etc.)?	Yes
26	Are all Applications that host sensitive Information fully supported by the software provider?	Yes
27	Are all software application and security patches evaluated, tested prior to deployment?	Yes
28	Are security mechanisms in place to protect access to the company's data?	Yes
29	Do you enforce password complexity requirements?	Yes

Croner
HR · Tax · H&S · Reward

No	Data Security	Y/N
30	Are passwords changed on a regular basis?	Yes
31	Are idle time screensaver locks enforced for all staff?	Yes
32	Can you confirm that all default admin and application backdoor accounts have been removed?	Yes
33	For systems which are accessible to users from the Internet are precautions taken to prevent the existence and exploitation of web application vulnerabilities such as cross-scripting or SQL Injection.	Yes
34	Is remote access secured?	Yes
35	Is sensitive data encrypted in databases?	Yes
36	Are all new laptops encrypted?	Yes
No	Backup System	Y/N
37	Is data backed up daily?	Yes
38	Is access to backup data secured?	Yes
39	Is resilience built into all key systems?	Yes
40	Is the data restore process tested?	Yes
41	Are measures in place to ensure data integrity and continuity?	Yes
No	Retention/Disposal	Y/N
42	Do you have a data retention/deletion policy that applies to personal data?	Yes
43	Are there any circumstances in which a copy of any personal data is stored after the end of the services?	Yes

Croner
HR · Tax · H&S · Reward

No	Cloud Services & 3rd Party Access	Y/N
44	Does your organisation use Secure Cloud Storage facilities for processing data?	Yes
45	Is security maintained and tested regularly?	Yes
46	Does all data reside in the EU?	Yes
47	Are all contractual IT Security Requirements in place with third parties and GDPR compliant?	Yes
48	Do you have in place with third parties written contracts including conditions requiring compliance with Data Privacy legislation?	Yes

Additional information is available to clients upon request.