ROSS CONSULAR SERVICES LIMITED

COMPLIANCE TO GDPR

COLLECTION OF DATA:
Data is received either by Post, collection from our Client / Third Parties premises, delivered directly to us or via email.

STORAGE AND LOCATION OF DATA:
Hard copies of documents are kept in a secure safe overnight. Electronic information is stored on our secure in-house server. Our offices are also alarmed with shutters on all downstairs windows and outside doors. Internal doors are locked overnight.

DISCLOSURE:
Information will be passed to one or all of the entities listed below as required to process your request.
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller as per GDPR article 6 1 (e).

DATA PROCESSING:
Information supplied to us is checked and documents prepared in our offices before being passed to some or all of the various entities as listed below.

Once the information has been passed to an Entity we have no control over what they do with the information thereafter.

DATA RETENTION AND DELETION:

VISAS
All visa applications/paperwork received pertaining to visas are submitted to the various Entities as required. We do not keep any personal data except what is shown on our order form which is the name of the applicant, date of Birth and their passport number. Extra paperwork not required by them is either returned to the applicant or shredded at our premises. When the work is completed the order forms are scanned onto a secure database and kept for 12 months thereafter they are removed from our system. The exception being applications for Saudi Arabia as the Embassy insist that the information is kept by us for 2 years. This information is kept on an encrypted key within the Company safe.

DOCUMENTS
Export / Legal Documents are all scanned onto a secure database before going to the various entities below. All additional paperwork not required is returned to the Client on completion of the work. All paperwork is deleted after 12 months.

RECEIVING PAYMENT:
We do not take online payments or retain credit/debit card details.

Payment can be received via: BACS, Credit/Debit card in person or via the phone.
We discourage credit/debit card details being sent to us by email or in the post. If however this occurs the information is immediately deleted from our system upon payment being taken.

All credit/debit card details are destroyed by this office once payment has been made.

Entities:
Local / Arab Chamber of Commerce, Notary Public, Foreign Office, Translator, Embassy / Consulate, Passport Office

ROSS CONSULAR SERVICES LIMITED

May 2018

GDPR Data and IT Security Risk Assessment

Ref	Question	Yes	No	N/A	Supporting information
	Section 1. Roles and Responsibilities				
1.1	Do you regularly, and in any event not less than once in every year, measure, review and report to your Clients your compliance with your IT security obligations detailed in the contract?		✓		Can be done upon request
1.2	Do you undertake regular security risk assessments (and in any event not less than once every 12 months) and take steps as required to mitigate the risks identified?	✓			
1.3	Do you clearly define appropriate IT Security related roles and responsibilities for your personnel, including the limitations of each role and the level of training required?	✓			
1.4	Do you annually obtain and record from each of your personnel an acknowledgement that they understand their IT Security related responsibilities for the provision of the Services?			✓	
1.5	Before providing access to your Clients Data or Confidential Information, do you provide training to all personnel engaged in the provision of the services covering roles, responsibilities, processes and controls for handling and protecting your Clients Data and Confidential Information?	✓			
1.6	Are all personnel subject to a testing component to confirm that they understand the meaning of security awareness and the importance of protecting the confidentiality, integrity and availability of your Clients Data and your Clients Confidential Information and your systems?			✓	
1.7	Are personnel annually recertified and their training record updated?			✓	
1.8	Did you appoint a security manager prior to commencement of services to your Clients to act as a single point of contact to your Clients for security related matters?	✓			
	Section 2. Security Incidents				
2.1	Do you make all reasonable efforts to immediately (or within a maximum of 24 hours) inform your Clients of an actual or potential Security Incident relevant to the services being provided to your Clients?	✓			
2.2	Do you have an Incident Management Process that is documented, approved by Compliance and Management and monitored?		✓		
2.3	Are all Incidents and Security Incidents managed, documented, reviewed and resolved in accordance with the agreed Incident Management Process?			✓	
2.4	Do you have a process for dealing with incidents that require forensic investigation, including the ability to analyze and preserve evidence in a forensically sound manner to support criminal proceedings if required?			✓	
	Section 3. Third Parties and Sub-Contractors				
3.1	Do all agreements with Sub-contractors and other Third Parties upon whom you are reliant to provide the services, include a right for you and your Clients (or its Agents) to jointly and independently conduct a security review for the purposes of ensuring they are meeting the		✓		Third Parties/Sub-contractors are Government Bodies and Embassies who do not allow anybody to access their

Ref	Question	Yes	No	N/A	Supporting information
	obligations under the terms of your contract with your Clients?				security systems. Our IT people would allow access to us to review security but discussions would be needed for Clients to have access.
	Section 4. Security Assessments				
4.1	Do you engage a Security Assessment Vendor to perform a Security Assessment on at least an annual basis (consisting of what is commonly known as a 'Penetration Test')?			✓	Small Business
4.2	Where applicable to the service provided, do you periodically (at least annually) test the software code and other aspects of the Application Service Provider (ASP) product, the ASP system and the Services for potential areas where security could be breached?	✓			The software has access controls and any changes made to these mechanisms are tested at the time. The IT provider is notified of any issues identified by the user during testing and subsequent use of the systems they provide.
	Section 5. Information Security Governance				
5.1	Do you have a documented information security management framework which is approved by Senior Management?	✓			
5.2	Is the information security status of critical IT environments, applications, computer installations, networks and systems development activity supporting the services subject to thorough, independent and regular security audits/reviews?	✓			
	Section 6. Information Security Policy				
6.1	Do you have a comprehensive, documented Information Security Policy?	✓			
6.2	Is your Information Security Policy communicated to all members of your personnel and all other Third Parties with access to your Clients Data, your Clients Confidential Information, your information or systems (where such Third Parties have been pre-approved in writing by your Clients before such access has been granted)?			✓	
	Section 7. Asset Controls				
7.1	Do you maintain a complete and accurate inventory of essential information about hardware and software (e.g. unique identifiers, version numbers and physical locations) and keep this up to date?	✓			
7.2	Have you documented and implemented a data classification process for all system and business processes handling your Clients Data or Confidential Information or used to provide services to your Clients?	✓			
7.3	Is all of your Clients Data and Confidential Information held or transported on data storage media (including laptop computers, PDAs, portable disk drives, magnetic tapes, memory sticks, and CD's)	✓			

Ref	Question	Yes	No	N/A	Supporting information
	encrypted and protected against corruption, loss or disclosure?				
7.4	Is all backup and archival media containing your Clients Data and Confidential Information, or other information used to provide the services, contained in secure, environmentally-controlled storage areas owned, operated, or contracted for by you?	✓			
7.5	Does the secure destruction of redundant computer equipment and media include the secure erasure of information when it is no longer required such that the information cannot be retrieved (including magnetic tapes, disks, CDs and stationery)? – If Yes – please state method used.	✓			
7.6	Prior to disposal, is printed Client Data and Confidential Information properly shredded on shredding machines placed within the facilities in which the Client Confidential Information and Client Data is located? If yes please state Security level e.g DIN 66399 P1-P7	✓			DIN 66399 P2
	Section 8. Identity and Access control				
8.1	Are all personnel with access to your system authenticated via user IDs and passwords or by strong authentication mechanisms (e.g. smart cards, biometric devices or other two-factor authentication mechanisms) before they can gain access to systems and applications?	✓			
8.2	Does your system(s) adequately provide the following security measures:				
	• Authentication credentials of the previous user do not appear on the logon prompt or anywhere else that is visible?		✓		
	• The system restricts the number of unsuccessful sign-on attempts to prevent password guessing attacks?	✓			
	• Sessions are restricted or timed out after a defined period of inactivity which in any event is not greater than 30 minutes?		✓		Screens lock after 5 minutes
	• Re-authentication of users occurs after session timeout or interruption?		✓		Password required to unlock
8.3	Do you ensure that authentication data such as passwords are not stored in a form that allows the authentication data to be recovered in readable or decipherable form?	✓			
8.4	Do you ensure that password complexity controls are implemented to ensure that all passwords include a combination of character classes and minimum length that is sufficient to prevent exhaustive or dictionary attacks?	✓			
8.5	Do you ensure all passwords and other authentication credentials (eg, tokens) are set and communicated only using a secure and controlled process?	✓			
8.6	Does the password reactivation process ensure that passwords are only released to authorised individuals? [Note: This question applies to both IT systems and infrastructure]	✓			
8.7	Does the password reactivation process ensure that a record of the re-activation of, or password release for, system and generic or shared accounts is maintained? [Note: This question applies to	✓			

Ref	Question	Yes	No	N/A	Supporting information
	both IT systems and infrastructure]				
8.8	Do you ensure the following for generic or shared accounts created by systems or infrastructure (e.g. root, administrator):				
8.9	The accounts are not used by individuals interactively unless absolutely necessary?	✓			
8.10	Use of the accounts is subject to documented approvals (irrespective of whether your Client or your personnel approve such access)?	✓			
8.11	Use of the accounts could only be attributable to an authorised individual?	✓			
8.12	Use of the accounts is limited to a specific authorised activity for a specific authorised timeframe?		✓		
8.13	Passwords for the accounts are changed following use, and as a minimum every six months?	✓			
8.14	Do you keep a record of all accounts and their owners, and appoint a new account owner if an existing owner leaves?	✓			
	Section 9. System/Application Configuration				
9.1	Are host systems and network devices forming part of your systems configured to function in accordance with Good Industry Practice, applicable specifications and functionality requirements, including preventing unauthorised or incorrect updates being applied to such systems and network devices?	✓			
9.2	Are security controls developed and implemented to restrict remote access to your systems to only authorised individuals and to ensure that remote access user activity is logged and subject to review?	✓			
	Section 10. System/Application Monitoring				
10.1	Do you maintain logs of all key events, such as those that have the potential to impact the confidentiality, integrity and availability of the service to your Clients and that may assist in the identification or investigation of material incidents and/or breaches of access rights occurring in relation to your systems? [Note: Where applicable, key events also include the use of generic or shared default accounts that provide a user privileged access to IT infrastructure.]	✓			
10.2	Is the scope of logging (including events which are to be captured by system type) documented and reviewed at least annually, and does this specify the logs which must be subject to review, the frequency of the review, the individuals responsible for the review, and the procedure for reporting the subsequent results and storing the logs?	✓			
10.3	Are logs of key events stored and transmitted securely (i.e. to avoid unauthorised access or tampering)?	✓			
10.4	Are logs of key events kept for at least 12 months (or as otherwise specified in the contract)?		✓		

Ref	Question	Yes	No	N/A	Supporting information
10.5	Do you review the logs of all key events within your systems (preferably using automated tools)? [Note: Where applicable, key events also include the use of generic or shared default accounts that provide a user privileged access to IT infrastructure.]	✓			
10.6	Do you enforce a segregation of duties in the review process, such that the same individual is not responsible for reviewing a log of their own actions? [Note: This question applies for access to both IT systems and infrastructure]		✓		Small Business
10.7	Upon identification of any material incidents and/or breaches of access rights do you ensure that the Incident Management Process is followed? [Note: This question applies for access to both IT systems and infrastructure].			✓	
10.8	Do you deploy intrusion detection tools in your systems to identify suspected or actual attacks and respond in accordance with Good Industry Practice?		✓		Changes to implement these measures are under discussion
10.9	Do you deploy data leakage tools, in accordance with Good Industry Practice, to detect any unauthorised transfers of your Clients Data and Confidential Information within your systems and any unauthorised external transfers of your Client Data and Confidential Information?		✓		Changes to implement these measures are under discussion
	Section 11. Network Security				
11.1	Is your network protected using all available in-built security controls?	✓			
11.2	Is your network supported by accurate, up-to-date diagrams and by documented control requirements and procedures?	✓			
11.3	Are all external connections to your networks and applications individually identified, verified, recorded, and approved by you in accordance with your Information Security Policy and Good Industry Practice?	✓			
11.4	Are all traffic networks not owned or managed by you routed through a firewall, prior to being allowed access to your network?	✓			
11.5	Do you ensure that wireless access to your systems is subject to authorization, authentication and encryption protocols consistent with Good Industry Practice?	✓			
11.6	Do you protect electronic communications (such as e-mail and instant messaging) using a combination of policy, training, and procedural and technical security controls?	✓			
	Section 12. Encryption processes and Policies				
12.1	Do you ensure all cryptographic keys are managed securely at all times, and in accordance with documented control requirements and procedures which are consistent with Good Industry Practice?	✓			
12.2	Do all cryptographic keys used to protect your Client data exist only in one of the following formats? In a tamper-responsive security module, encrypted or in component form under the principles of split knowledge and dual control	✓			

Ref	Question	Yes	No	N/A	Supporting information
12.3	Are controls in place to protect secret keys by:				
	• Preventing disclosure of keys throughout their lifetime?	✓			
	• Detecting attempted use of any key for other than its intended purpose?	✓			
	• Preventing or detecting the unauthorised modification, use, substitution, deletion or insertion of any key?	✓			
12.4	Are keys generated using devices and processes designed and/or certified for random number generation which make it impossible to predict a resultant key value?			✓	
12.5	Is there a risk based key renewal schedule in place that is followed with finite lifetimes defined for all keys?			✓	
12.6	Are controls in place which;				
	• Require revocation of a key if compromise is known or suspected?	✓			
	• Require keys to be generated independently of any compromised keys?			✓	
	• Segregate keys to prevent any single compromise affecting multiple groups of parties?			✓	
12.7	Are all devices used for loading, generation, or key storage designed or certified as tamper responsive and are integrity and authenticity controls in place to protect the device throughout its lifetime?	✓			
	Section 13. Malware Protection				
13.1	Have you established and do you maintain up-to-date protection against Malicious Code throughout your business?	✓			
13.2	Where updates cannot be applied to a system, do you deploy appropriate security countermeasures to protect the vulnerable systems?	✓			
	Section 14. System/Application Development				
14.1	Are development activities (including those undertaken by any Sub-contractors) carried out in accordance with a documented secure system development methodology which includes definition and testing of security requirements and specification of secure coding practices?		✓		The IT company utilise secure system development methodologies but they are not formally documented. However, this is something they are considering doing.
14.2	Are system development activities performed in specialized development environments, isolated from the live environment, and protected against disruption and disclosure of information?	✓			Development is performed on our IT companies systems only.
14.3	Are all elements of your systems tested at all stages of the systems development lifecycle before the system is promoted to the live environment?	✓			
14.4	Do you ensure that live data (including Personal Data) is not used within test environments without your Clients prior written approval and agreement of the controls to be implemented to	✓			All test data is anonymous

Ref	Question	Yes	No	N/A	Supporting information
	protect that live data?				
14.5	Do you install new systems in the live environment in accordance with a documented installation process?	✓			
	Section 15. Change and upgrade Management				
15.1	Are changes to any part of your systems tested, reviewed and applied using a documented change management process?	✓			Carried out by our IT provider
15.2	Are emergency fixes, security patches and other relevant security vulnerability updates implemented when available and approved, unless this introduces higher business risks?	✓			
15.3	If for any reason your systems cannot be updated do you have security measures installed to fully protect the vulnerable system?	✓			
15.4	Do you have a documented process to identify and remediate security vulnerabilities in the software provided to your Clients and provide these updates to your Clients immediately upon their becoming available?			✓	
	Section 16. Third Party Management				
16.1	Are all connections from Third Parties subject to a risk assessment, approved and agreed by both parties in a documented agreement, such as a contract?			✓	
16.2	Are services required to support the Services provided to your Clients only obtained from service providers capable of providing security controls no less rigorous than those you are required to comply with under your contract with your Clients?	✓			
16.3	Are all such services from Third Parties provided under appropriate contracts?	✓			
	Section 17. Logical Access Management				
17.1	Do you have a logical access management policy and procedure in place that applies to your Clients Data?	✓			
17.2	Do you ensure that all Supplier Personnel who may have access to your Clients Data are aware of all relevant logical access management policies?	✓			
17.3	Do you have formal policies and procedures in place covering:				
	• Starter/ mover/ leaver processes covering all permanent and temporary staff, guests and contractors and which require documented approvals before access is granted, re-enabled or changed? [Note: This question applies to both IT systems and infrastructure]	✓			
	• Reactivation of locked/disabled accounts? [Note: This question applies to both IT systems and infrastructure]	✓			
17.4	Performing regular reviews of access granted to your Clients Data or IT infrastructure supporting your Clients applications, to ensure the level of access granted is appropriate (often referred to as	✓			Full IT system reviews annually by our IT provider

Ref	Question	Yes	No	N/A	Supporting information
	"Recertification")?				
17.5	Implementing segregation of duties based upon the concept of 'least privilege' (e.g., granted on the basis of roles or profiles)? [Note: This question applies to both IT systems and infrastructure]	✓			
17.6	Granting and Revoking of privileged user access to IT systems and, where applicable, infrastructure?	✓			
17.7	Ensuring that privileged user access accounts are not provided for use in day to day operations?	✓			
17.8	Ensuring that privileged user access accounts are terminated as soon as possible, and no later than 24 hours, following the user leaving employment or ceasing to fulfill that role? [Note: This question applies to both IT systems and infrastructure]	✓			
17.9	Ensuring that developers are only granted access to production systems for planned and emergency change support purposes?	✓			
17.10	Do you ensure that individuals cannot authorise their own access and user account administrators that create, modify or revoke a user account are not involved in the authorisation process? [Note: This question applies to both IT systems and infrastructure]	✓			
17.11	Do you maintain an audit trail of the creation, modification and revocation of accounts? [Note: This question applies to both IT systems and infrastructure]	✓			
17.12	Does the recertification process ensure that the access rights of all users are appropriate and have been authorised? [Note: This question applies to both IT systems and infrastructure]			✓	
17.13	Does the recertification process ensure that all accounts, including system and generic or shared accounts, are reviewed to assess their continued requirement? [Note: This question applies to both IT systems and infrastructure]			✓	Not Recertification, but user account status is reviewed on a quarterly basis
17.14	Do you produce documentary evidence as part of the recertification process, which includes the recording of issues identified and subsequent actions taken to address those issues (e.g. account removal)? [Note: This question applies to both IT systems and infrastructure]	✓			
17.15	Do you ensure all accounts are used by a sole, identifiable individual? (Excluding any shared or generic accounts used to access the systems for which your Clients have provided prior written approval.)	✓			
17.16	Where your Client approves the use of shared or generic accounts to access the systems, do you keep a record of all users of those generic or shared accounts?			✓	
17.17	Do you ensure all accounts are disabled promptly when no longer required for the performance of your obligations under the contract (or upon request from your Clients)?	✓			
17.18	Do you ensure all users of systems are warned of the legal consequences of unauthorised access? (e.g. prior to logging on to the systems)			✓	