

Supplier Data & Security Questionnaire

Data Protection Officer

Question	Supplier response
What is the name and contact details of your Data Protection Officer?	Tanya Warnford-Davis gdpr-officer@prospectsoft.com

Accreditations

Question	Supplier response
What security accreditations you have?	ISO 27001

Systems and applications

Please refer to our published Terms & Policies [here](#).

Business continuity

Question	Supplier response
Do you have a business continuity plan that is reviewed, tested and updated at least annually?	Yes, it is tested at least once every 6 months.

User access

Question	Supplier response
Who within your organisation will have access to the personal data?	Access is restricted to staff involved in supporting customers.
What user authentication do you use on networks/systems that store/process our data?	Azure AD with MFA where appropriate.
Do you have a password complexity policy?	Yes, we have a password policy as part of our ISO 27001 ISMS.

Penetration / security testing

Question	Supplier response
Do you conduct penetration testing at least annually on all networks hosting our data?	Independent automated systems monitor every aspect of our solution, from secure certificate expiry to the performance of individual services. We use independent experts to actively scan and report on PCI vulnerability tests and to perform regular network and software penetration testing.

Physical security

Question	Supplier response
Please describe the physical security that protects our data, including building access and physical server access.	Prospect 365 runs on the Microsoft Azure Cloud. Microsoft has adopted ISO 27018, the international cloud privacy standard and conforms to the latest EU privacy laws. All other suppliers have adopted ISO 27001 or are in the process of being replaced by suppliers who do. Our Building security is compliant with ISO 27001.

Application development

Question	Supplier response
Do you have policies for secure software development?	Please refer to our published Terms & Policies here .
Are production systems used in test or development process?	No, we have entirely separate production, QA and development environments.

Logs

Question	Supplier response
Do you keep and regularly review access, event, error and transaction logs on all networks storing/processing our data?	All Prospect 365 customer data access and usage is logged and monitored by Microsoft Application Insights.
Are all logs protected from deletion and/or amendment?	They are protected for 7 days, after which they are automatically deleted.
Is access to these logs restricted?	Yes, restricted only to staff who need access.

Breach notification

Question	Supplier response
Do you have a formal breach notification process?	Yes
Detail the timelines to notify us of any suspected breach.	We would notify you without undue delay.
Have you had a security breach within the last 12 months? If so, please describe the incident, effect and outcome.	No

Data retention / deletion

Please refer to our published Terms & Policies [here](#).

Data encryption

Please refer to our published Terms & Policies [here](#).

Territories

Question	Supplier response
Is any of our data processed, stored or transferred outside of the EEA?	Data is held within the EEA or by companies covered by the Data Privacy shield.

Sub-processors

Question	Supplier response
Is our data passed on to any third parties for processing?	Only with consent and to fulfil our contractual obligations. Sub-Processors undergo due diligence to ensure they comply with and uphold GDPR.