DATA PROTECTION SURVEY

Please complete this survey and provide copies of any relevant documentation if you process personal data on our behalf.

Question	Reply
Do you employ a data protection officer or similar individual dedicated to data privacy matters within your organisation? If so, please ask them to complete this survey; otherwise please complete the survey to the best of your knowledge and with help from your legal or compliance department, as appropriate.	
Please describe what personal data you handle / will handle on our behalf. Personal data is data relating to an identified or identifiable natural person, such as names, addresses, email addresses, positions held, images, video footage, job applications, personnel files, occupational health records, opinions about individuals, correspondence. It will also include data that may indirectly identify an individual, such as a cookie data, user id, anonymous behavioural data, address without a name, etc.	
Please describe what special category data you handle / will handle on our behalf, if any. Special category data includes data revealing a person's racial and ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data (e.g. fingerprints or facial recognition) and genetic information, information about a person's health, sex life and sexual orientation, and data relating to criminal convictions or offences.	
Do you know if you act / will act as a controller or processor in respect of our personal data? A controller is a party that determines the purposes (that is, why information is being processed) and means (that is, how information is being processed) of processing. A processor is a party that processes personal data on behalf of a controller (if you are a processor, we may be the controller).	
Do you / will you transfer our personal data outside the UK or EEA? E.g. if you, your servers or contractors are based outside the UK or EEA.	
Describe how you process / will process our personal data in connection with your services. E.g. you store data in a cloud and make data available to our users via online portal. E.g. you carry out calculations for payroll purposes and issue payslips to our employees. E.g. you analyse our customer interactions and provide reports. E.g. you serve ads to our customers' devices based on user profiles built from behavioural data.	
Do you / will you use our personal data for any other purposes? E.g. your own internal purposes such as anonymised data used for business analytics.	
Please provide copies of any data protection policies that you have in place. E.g. Data protection policy, information security including access control, data retention policy for customer data, etc.	

Question	Reply
Do you / will you engage any contractors or service providers who further process / will further process our personal data? If so, which ones? E.g. you use a third party cloud provider to store our data. E.g. you use third party tools to analyse our data. E.g. you employ onsite contractors who handle our data.	
Has there been, or do you anticipate, any change in your service that means that you will use more of our personal data? E.g. new functionality in your service, restructuring of your team, use of new systems, etc.	
Please provide a list of your technical and administrative security measures deployed to safeguard our data. E.g. copy of your information security policy, AUP, BYOD, security handbook, security specifications schedules, SOC or ISO27001 reports, encryption used to safeguard RF data in transit and at rest, etc.	
Are your personnel subject to vetting, obligation of confidentiality and data protection training? E.g. contract of employment with confidentiality clause, separate NDAs are executed, background check provider is used for a quick screening of successful job candidates, annual information security training provided to employees, etc.	
Would it be possible for you to use pseudonymised or anonymous data instead of personal data? E.g. instead of handling the names of our users, could you assign user IDs and keep the list of names separate from the user IDs in order to enhance security?	
Who has / will have access our personal data and why? How do you ensure access control? I.e. measures to ensure that only those of your personnel with a genuine need to know have access to the personal data.	
What records do you / will you keep about our personal data? E.g. computer logs, lists with user privileges, records showing who accessed the data, when, what changes were made, or what data was deleted, a record of processing activities, etc.	
How do you / will you keep our data up to date? E.g. is there a procedure or policy to update data as and when changes become known or do you regularly check for changes?	
Have any of our personal data you hold become obsolete or superfluous? Do you purge our personal data if they are no longer needed? E.g. is there a procedure or policy to delete inactive data automatically or manually?	

Question	Reply
Can you ensure that all personal data are erased or returned at the end of the service? E.g. unless you have a legal obligation or business reason to retain such data. Please specify the reason for any such continued retention.	
What procedure do you have in place to report personal data breaches to us without delay? Have you had any personal data breaches over the last 12 months and how were they resolved? Personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, such as, accidentally sharing data with a third party, data theft by employee, lost data stick, infiltration of network by cyber criminals, etc.	
Do you have / will you have direct contact with our data subjects (e.g. our customers or employees) or do you / will you operate in the background unknown to data subjects? E.g. our users can access your portal online; you contact our customers by email or phone; our users get in touch with you to seek services.	
How do you deal with personal data related requests from individuals? How many requests have you received in the last 12 months? E.g. access request, erasure request.	
How do you deal with data related requests from authorities? How many requests have you received in the last 12 months? E.g. regulatory or court requests.	
Do you carry out data protection impact assessments when appropriate? E.g. a process where relevant stakeholders consider how any business processes may impact on individuals' data privacy rights, considering the lawfulness of such processing and finding solutions on minimizing any such impact.	